マルチレイヤー･モジュラー･スイッチ

SwitchBlade® 7800S
SwitchBlade® 5400S

SB-7800S・SB-5400S ソフトウェアマニュアル

解説書 Vol.1

Ver. 10.7 対応

613-000107 Rev.J 080731

■対象製品

このマニュアルは SB-7800S および SB-5400S を対象に記載しています。また，SB-7800S のソフトウェアおよび SB-5400S のソフトウェアいずれも Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SW および各種オプションライセンスによってサポートする機能について記載します。

■日本国外での使用について

弊社製品を日本国外へ持ち出されるお客様は、下記窓口へご相談ください。
TEL: 0120-860442
月～金（祝・祭日を除く）9:00 ～ 17:30

■商標一覧

SwitchBlade は，アライドテレシスホールディングス（株）の登録商標です。
Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，米国 Xerox Corp. の商品名称です。
GSRP は，アラクサラネットワークス（株）の商標です。
HP OpenView は米国 Hewlett-Packard Company の米国及び他の国々における商品名称です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
NavisRadius は，Lucent Technologies 社の商標です。
NetFlow は米国およびその他の国における米国 Cisco Systems, Inc. の登録商標です。
Octpower は，日本電気（株）の登録商標です。
Odyssey は，米国 Funk Software Inc. の米国における登録商標です。
sFlow は米国およびその他の国における米国 InMon Corp. の登録商標です。
Solaris は，米国及びその他の国における Sun Microsystems, Inc. の商標又は登録商標です。
UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■電波障害について

この装置は，情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

■高調波規制について

高調波電流規格　JIS C 61000-3-2 適合品
適合装置：
SB-7804S-AC
SB-7808S-AC
SB-7816S-AC
SB-5402S-AC
SB-5404S-AC

■ご注意

■マニュアルバージョン

2005 年 3 月 Rev.A 初版
2005 年 7 月 Rev.B
2006 年 1 月 Rev.C
2006 年 4 月 Rev.D
2006 年 6 月 Rev.E
2006 年 8 月 Rev.F
2007 年 6 月 Rev.G
2008 年 3 月 Rev.H
2008 年 7 月 Rev.J

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは SB-7800S および SB-5400S モデルを対象に記載しています。また，SB-7800S のソフトウェアおよび SB-5400S のソフトウェア，いずれも Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SW および各種オプションライセンスによってサポートする機能について記載します。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

なお，このマニュアルでは特に断らないかぎり SB-7800S と SB-5400S に共通の機能について記載しますが，どちらかの機種固有の機能については以下のマークで示します。

【SB-7800S】：

SB-7800S でサポートする機能です。SB-5400S はサポートしない機能または該当しない記述です。

【SB-5400S】：

SB-5400S でサポートする機能です。SB-7800S はサポートしない機能または該当しない記述です。

また，このマニュアルでは特に断らないかぎり基本ソフトウェア OS-SW の機能について記載しますが，各種オプションライセンスでサポートする機能を以下のマークで示します。

【OP-BGP】：

SB-7800S と SB-5400S のオプションライセンス OP-BGP でサポートする機能です。

【OP-ISIS】：

SB-7800S と SB-5400S のオプションライセンス OP-ISIS でサポートする機能です。

【OP-MLT】：

SB-7800S と SB-5400S のオプションライセンス OP-MLT でサポートする機能です。

【OP-ADV】：

SB-7800S と SB-5400S のオプションライセンス OP-ADV でサポートする機能です。

【OP-OSPF(SB-5400S)】：

SB-7800S では基本ソフトに含む機能ですが，SB-5400S はオプションライセンス OP-OSPF でサポートする機能です。

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■対象読者

SB-7800S または SB-5400S を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■マニュアルの構成

「SB-7800S・SB-5400S ソフトウェアマニュアル　解説書」は Vol.1 および Vol.2 に分かれています。

「SB-7800S・SB-5400S ソフトウェアマニュアル　解説書 Vol.1」は，次に示す編と付録から構成されています。

第 1 編　概要
SB-7800S および SB-5400S の概要について説明しています。

第 2 編　収容条件
SB-7800S および SB-5400S の収容条件について説明しています。

第 3 編　ネットワークインタフェース
イーサネットなど SB-7800S および SB-5400S がサポートしているネットワークインタフェースについて説明しています。

第 4 編　レイヤ 2 スイッチ
SB-7800S および SB-5400S がサポートしているレイヤ 2 スイッチについて説明しています。

第 5 編　レイヤ 3 インタフェース
SB-7800S および SB-5400S がサポートしているレイヤ 3 インタフェースについて説明しています。

第 6 編　IPv4 ルーティング
IPv4 ネットワークでのパケット中継およびルーティングプロトコルについて説明しています。

第 7 編　IPv6 ルーティング
IPv6 ネットワークでのパケット中継およびルーティングプロトコルについて説明しています。

付録 A　準拠規格
準拠している規格について説明しています。

付録 B　謝辞 (Acknowledgments)
謝辞 (Acknowledgments) を掲載しています。

付録 C　用語解説
このマニュアルで使用している用語の意味を説明しています。

■読書手順
このマニュアルは次の手順でお読みいただくことをお勧めします。

収容条件を知りたい
IPルーティング機能を知りたい
IPv6の機能を知りたい
運用機能を知りたい
レイヤ2スイッチ機能を知りたい
QoSの機能を知りたい
解説書 Vol.1
第１編　概要
1．本装置の概要
2．装置構成
第２編　収容条件
3．収容条件
第３編 ネットワークインタフェース
4．イーサネット
5．POS
第４編　レイヤ2スイッチ
6．レイヤ2スイッチ
7．VLAN
8．スパニングツリー
9．IGMP snooping/MLD snooping
第５編　レイヤ3インタフェース
10. レイヤ3インタフェース
第６編　IPv4ルーティング
11．IPv4パケット中継
12．RIP/OSPF
13．BGP4
14．IS-IS
15．IPv4マルチキャスト
第７編　IPv6ルーティング
16．IPv6パケット中継
17．RIPng/OSPFv3
18．BGP4+
19．IPv6マルチキャスト
付録
解説書 Vol.2
第１編　QoS
1．QoS制御機能
2．Diff-serv機能
第２編　レイヤ2認証
3．IEEE 802.1X
第３編　高信頼性機能
4．冗長構成
5．GSRP
6．VRRP
7．CP輻輳制御
8．IEEE802.3ah/UDLD
第４編　運用
9．SNMPを使用したネットワーク管理
10．フロー統計を使用したネットワーク管理
11．隣接装置情報の管理
12．ポートミラーリング
13．RADIUS/TACACS+
14．運用機能
第５編 システム構築のためのポイント
15．他機種との接続
16．網・各種専用線サービスとの接続
付録
(凡例)
：必ず読む項目
：必要に応じて読む項目

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，あわせてご利用ください。
http://www.allied-telesis.co.jp/

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●ハードウェアの構成，およびソフトウェアの機能を知りたい

解説書 Vol.1
(613-000107)

解説書 Vol.2
(613-000108)

●ハードウェアの設備条件，取扱方法を調べる

SB-7800S
ハードウェア取扱説明書
(613-000105)

SB-5400S
ハードウェア取扱説明書
(613-000106)

●コンフィグレーションの作成方法，設定例

コンフィグレーションガイド
(613-000109)

コンフィグレーション
コマンドレファレンス Vol.1
(613-000111)

コンフィグレーション
コマンドレファレンス Vol.2
(613-000112)

●運用管理方法，トラブルシュート

運用ガイド
(613-000110)

→各コマンドの入力シンタックス，パラメータ詳細

運用コマンドレファレンス
Vol.1
(613-000113)

運用コマンドレファレンス
Vol.2
(613-000114)

→運用ログ詳細

メッセージ・ログレファレンス
(613-000115)

→MIB詳細

MIBレファレンス
(613-000116)

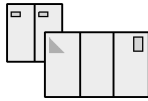
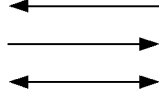
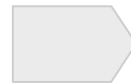
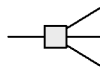
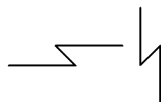
■このマニュアルでの表記

ABR	Available Bit Rate
AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AUX	Auxiliary
BCU	Basic management Control module
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic packet Switching module
BU	Basic control Unit
CBR	Constant Bit Rate
CDP	Cisco Discovery Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CP	multi layer Control Processor
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
Diff-serv	Differentiated Services
DIS	Draft International Standard/Designated Intermediate System
DLCI	Data Link Connection Identifier
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FCS	Frame Check Sequence
FDB	Filtering DataBase
FR	Frame Relay
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GFR	Guaranteed Frame Rate
GSRP	Gigabit Switch Redundancy Protocol
HDLC	High level Data Link Control
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IIH	IS-IS Hello
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
IS	Intermediate System
IS-IS	Information technology - Telecommunications and Information exchange between systems - Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface board
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
POH	Path Over Head
POS	PPP over SONET/SDH
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PSNP	Partial Sequence Numbers PDU
PSU	Packet Switching Module
PVC	Permanent Virtual Channel (Connection)/Permanent Virtual Circuit
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments

```
RIP         Routing Information Protocol
RIPng       Routing Information Protocol next generation
RM          Routing Manager
RMON        Remote Network Monitoring MIB
RPF         Reverse Path Forwarding
RQ          ReQuest
RSTP        Rapid Spanning Tree Protocol
SA          Source Address
SDH         Synchronous Digital Hierarchy
SDU         Service Data Unit
SEL         NSAP SELector
SFD         Start Frame Delimiter
SFP         Small Form factor Pluggable
SMTP        Simple Mail Transfer Protocol
SNAP        Sub-Network Access Protocol
SNMP        Simple Network Management Protocol
SNP         Sequence Numbers PDU
SNPA        Subnetwork Point of Attachment
SOH         Section Over Head
SONET       Synchronous Optical Network
SOP         System Operational Panel
SPF         Shortest Path First
SSAP        Source Service Access Point
STP         Spanning Tree Protocol
TA          Terminal Adapter
TACACS+     Terminal Access Controller Access Control System Plus
TCP/IP      Transmission Control Protocol/Internet Protocol
TLA ID      Top-Level Aggregation Identifier
TLV         Type, Length, and Value
TOS         Type Of Service
TPID        Tag Protocol Identifier
TTL         Time To Live
UBR         Unspecified Bit Rate
UDLD        Uni-Directional Link Detection
UDP         User Datagram Protocol
UPC         Usage Parameter Control
UPC-RED     Usage Parameter Control - Random Early Detection
VBR         Variable Bit Rate
VC          Virtual Channel/Virtual Call/Virtual Circuit
VCI         Virtual Channel Identifier
VLAN        Virtual LAN
VP          Virtual Path
VPI         Virtual Path Identifier
VPN         Virtual Private Network
VRRP        Virtual Router Redundancy Protocol
WAN         Wide Area Network
WDM         Wavelength Division Multiplexing
WFQ         Weighted Fair Queueing
WRED        Weighted Random Early Detection
WS          Work Station
WWW         World-Wide Web
XFP         10 gigabit small Form factor Pluggable
```

■図中で使用する記号の説明

このマニュアルの図中で使用する記号を，次のように定義します。

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外を使用しています。

- 宛て（あて）
- 宛先（あてさき）
- 迂回（うかい）
- 鍵（かぎ）
- 個所（かしょ）
- 筐体（きょうたい）
- 桁（けた）
- 毎（ごと）
- 閾値（しきいち）
- 芯（しん）
- 溜まる（たまる）
- 必須（ひっす）
- 輻輳（ふくそう）
- 閉塞（へいそく）
- 漏洩（ろうえい）

■ kB(バイト) などの単位表記について

1kB(キロバイト)，1MB(メガバイト)，1GB(ギガバイト)，1TB(テラバイト) はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

目次

第 1 編　概要

第 2 編　収容条件

第 3 編　ネットワークインタフェース

第４編　レイヤ２スイッチ

第 5 編　レイヤ 3 インタフェース

第 6 編　IPv4 ルーティング

第 7 編　IPv6 ルーティング

目次

解説書 Vol.2

第 1 編　QoS

第 4 編　運用

1 本装置の概要

本装置は電気，ガス，水道のような社会発展の基盤として，いつでも，どこでも，誰にでも安価，安心，安全，確実，便利に使えるライフライン・インターネットワークを提供します。この章では，本装置の特長について説明します。

1.1　本装置のコンセプト

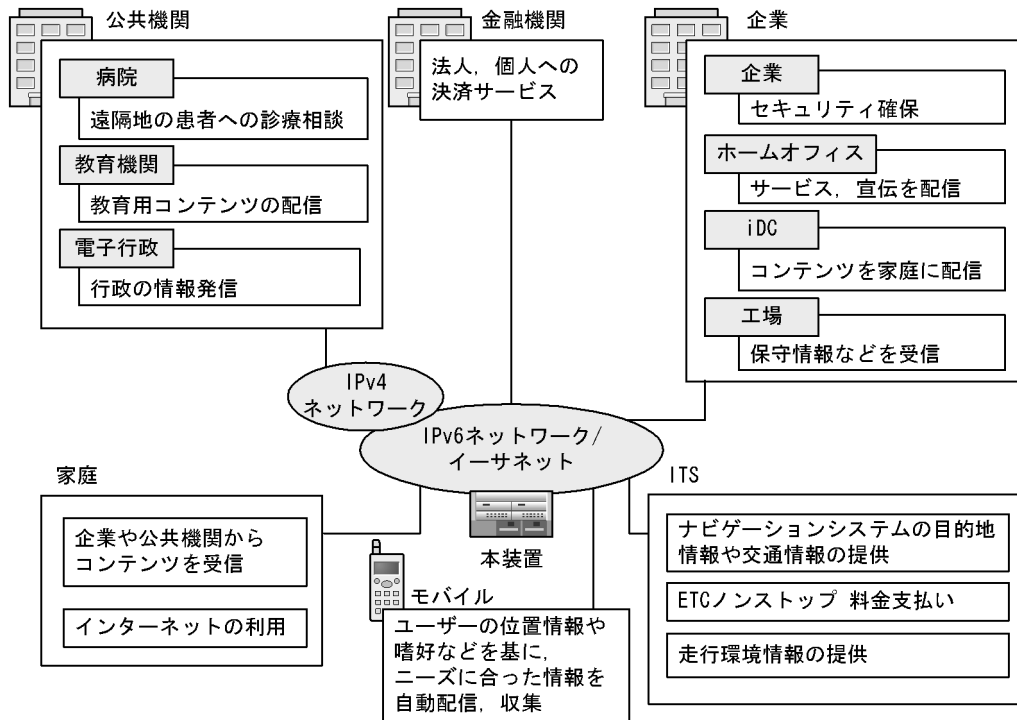
本装置は電気，ガス，水道のような社会発展の基盤として，いつでも，どこでも，誰にでも安価，安心，安全，確実，便利に使えるライフライン・インターネットワークを提供する高性能レイヤ 3 対応スイッチです。この章では，本装置の特長について説明します。

高信頼 IP/ イーサネット網は，本装置の次に示す技術によって実現します。

- どこでも使えるネットワーク
  - イーサネット (10Mbit/s ～ 10Gbit/s※) によるシームレス LAN・WAN 技術
  - IPv6 によるユビキタス・ネットワーク技術

  注※　SB-5400S では 10Mbit/s ～ 1Gbit/s になります。
- 必要なときに必要なだけ，確実に通信できる
  - 冗長構成による装置単体としての高信頼化，ホットスタンバイなどによるネットワークの高信頼性技術
  - 高速インタフェースできめ細かな QoS ／フィルタ制御技術
- 安全で安定した通信環境
  - フィルタリング，認証 (Radius) などのセキュリティ技術

本装置のコンセプトイメージを次の図に示します。

図 1-1　本装置のコンセプトイメージ

1.2　本装置の特長

本装置の特長のキーワードは，ミッションクリティカル対応の高い信頼性，バックボーン向けの高いスケーラビリティ，広域イーサネット網の仮想専用線の実現，多様なネットワークシステムへ適用するための充実したレイヤ 3 ルーティングとレイヤ 2 スイッチング機能を持つ高性能レイヤ 3 対応スイッチです。次にこれらのキーワードが示す本装置の特長について説明します。

1.2.1　ミッションクリティカル対応の高い信頼性

- **装置**
  高信頼設計，厳選した部品による装置自体の高信頼化と，実績ある安定したソフトウェア，厳しい製品品質検査基準により，きわめて高い製品信頼性を実現しています。また，電源部や共通部（バックプレーンスイッチ，CPU）の冗長構成によって高可用化を図れます。
- **ネットワークシステム**
  リンクや経路の高速切り替えを高速スパニングツリープロトコル (IEEE802.1w)，リンクアグリゲーション，VRRP，OSPF ECMP，GSRP(L2 スイッチ冗長化モジュール）によるロードバランスなどで実現します。
- **データ通信**
  イーサネット上で ATM 並みの QoS を実現するイーサネット QoS によってきめ細かな通信トラフィック制御を提供します。
- **保守運用**
  各種運用保守情報（運用ログ）の収集や運用保守情報のメール送信など，遠隔地からの稼働監視を実現します。

1.2.2　バックボーン向けの高いスケーラビリティ

低速な 10Mbit/s から高速な 10Gbit/s※までのイーサネットのインタフェースをサポートし，ワイヤレートでパケット転送します。

リンクアグリゲーション機能によって，必要に応じた回線帯域の増設ができます。例えば，1Gbit/s イーサネットを 2 本束ね 2Gbit/s の回線として使用できます。

注※　SB-5400S では 1Gbit/s までです。

1.2.3　充実したレイヤ 3 ルーティングとレイヤ 2 スイッチング機能

レイヤ 3 の機能として，本装置ではネットワークの規模に応じて利用できる複数のルーティングプロトコルをサポートしていますので，さまざまなネットワーク構成に対応できます。IPv6 のルーティングプロトコルは，先進のマルチキャスト (PIM-SM，PIM-SSM，MLD) や RIPng，OSPFv3，BGP4+，IS-IS，スタティックをサポートします。また，IPv4 のルーティングプロトコルは，RIP，OSPF，BGP4，IS-IS，スタティック，マルチキャストをサポートしますので，IPv4，IPv6 の多様なネットワークを構築できます。

レイヤ 2 機能としては，Tag-VLAN，ポート VLAN など各種 VLAN をサポートしています。スパニングツリープロトコルとして STP(IEEE802.1D)，RSTP(IEEE802.1w)，PVST+，MSTP(IEEE802.1s) をサポートします。

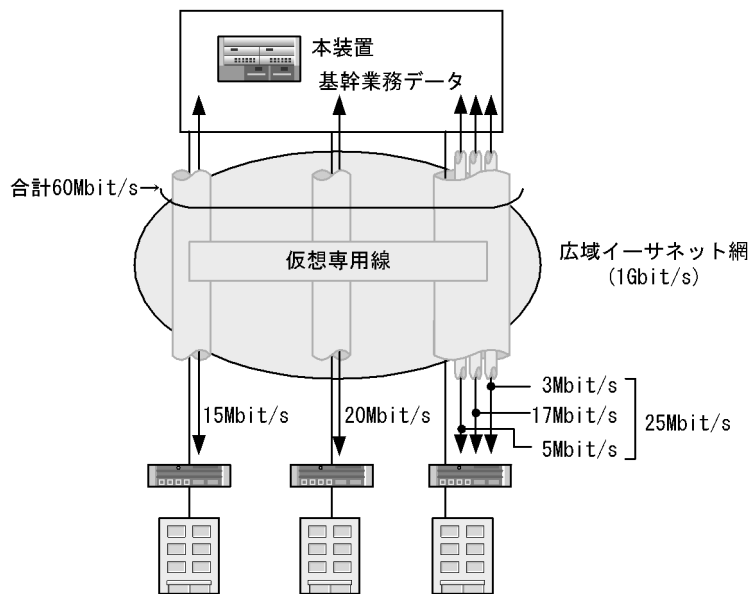
1.2.4　広域イーサネット網での仮想専用線の実現【SB-7800S】

SB-7800S では，階層化シェーパを使用して，広域イーサネット網で仮想専用線を実現できます。専用線，フレームリレー，ATM 回線から低料金・高速な広域イーサネット網へ容易に移行できます。

階層化シェーパの特長を次に示します。

- 契約帯域までシェーピングして契約帯域内でさらに 4 クラスの QoS 制御
- 1Gbit/s イーサネット上での VLAN とアプリケーションを意識したシェーピング
- きめ細かなパラメータ指定（パケットの L2 ヘッダ，L3 ヘッダ，L4 ヘッダの一部）
- 高いシェーピング精度（約数 % 以内）

階層化シェーパによる仮想専用線を次の図に示します。

図 1-2　階層化シェーパによる仮想専用線

1.3 本装置の機能

本装置を使用してできる機能を次の表に示します。なお，各機能が準拠している規格については「付録 A 準拠規格」を参照してください。

表 1-1 本装置の機能

分類		概要	説明している章
ネットワークインタフェース（IPv4，IPv6 共通）	イーサネット	• 10BASE-T/100BASE-TX/1000BASE-T • 1000BASE-X • 10GBASE-R【**SB-7800S**】 • 10GBASE-W【**SB-7800S**】 • リンクアグリゲーション • Tag-VLAN 連携	4 イーサネット
	POS	• OC-192c/STM-64POS • OC-48c/STM-16POS	5 POS（PPP Over SONET/SDH）【SB-7800S】
L2 機能	-	• トランスペアレントブリッジ	6 レイヤ 2 スイッチ
	VLAN	• ポート VLAN • IEEE802.1Q • tag- 変換 • プロトコル VLAN • MAC VLAN【**SB-7800S**】 • アップリンク VLAN • アップリンクブロック • プライベート VLAN	7 VLAN 8 スパニングツリー 9 IGMP snooping/MLD snooping
	スパニングツリー	• IEEE802.1D • IEEE802.1w • PVST+ • IEEE802.1s	
	-	• VLAN トンネリング	
	-	• IGMP snooping/MLD snooping	
付加機能		• フィルタリング • DHCPv4 リレーエージェント • DHCPv6 サーバ • マルチパス (ロードバランス) • ポリシールーティング	11 IPv4 パケット中継 16 IPv6 パケット中継
L3 機能 ルーティング	IPv4	• RIP，RIP2 • OSPF • BGP4 • IS-IS	12 RIP ／ OSPF 13 BGP4【OP-BGP】 14 IS-IS【OP-ISIS】
	IPv6	• RIPng • OSPFv3 • BGP4+ • IS-IS • トンネリング (IPv6 over IPv4 トンネル, IPv4 over IPv6 トンネル，6 to 4 トンネル)	17 RIPng/OSPFv3 18 BGP4+【OP-BGP】 14 IS-IS【OP-ISIS】 16 IPv6 パケット中継
マルチキャストルーティング	IPv4	• IGMP ver2，ver3 • DVMRP • PIM-DM • PIM-SM，PIM-SSM	15 IPv4 マルチキャスト【OP-MLT】
	IPv6	• MLD ver1，ver2 • PIM-SM，PIM-SSM	19 IPv6 マルチキャスト【OP-MLT】

分類	概要	説明している章
QoS，Diff-serv	• 契約帯域監視 • DSCP マーキング • LLQ+WFQ • 出力優先制御 • 均等保証 • 重要パケット保護 • WRED • UPC-RED • イーサネット帯域制御 (階層化シェーパ) **【SB-7800S】**	解説書 Vol.2　1. QoS 制御 解説書 Vol.2　2. Diff-serv 機能
認証	• IEEE802.1X	解説書 Vol.2　3. IEEE 802.1X
信頼性	• 環境モニタ • 自己診断 (MD) • 冗長構成 (電源，基本制御モジュール) • GSRP(レイヤ 2，レイヤ 3) • ホットスタンバイ (VRRP) • CP 輻輳制御 • IEEE802.3ah/UDLD	解説書 Vol.2　4. 冗長構成 解説書 Vol.2　5. GSRP 解説書 Vol.2　6. VRRP 解説書 Vol.2　7. CP 輻輳制御 解説書 Vol.2　8. IEEE802.3ah/UDLD
ネットワーク管理ほか	• SNMP ver1，ver2，ver3 • MIB-II，RMON，IP Forwarding MIB，Interface MIB，IPv6 MIB，プライベート MIB • フロー統計 (sFlow，NetFlow) • LLDP • OADP • ポートミラーリング	解説書 Vol.2　9. SNMP を使用したネットワーク管理 解説書 Vol.2　10. フロー統計を使用したネットワーク管理 解説書 Vol.2　11. 隣接装置情報の管理 解説書 Vol.2　12. ポートミラーリング
運用・保守	• 運用端末接続 • コンフィグレーション • ログイン認証 (RADIUS，TACACS+) • コマンド承認 (RADIUS，TACACS+) • アカウンティング (RADIUS，TACACS+) • オンライン中のボード交換 • 管理情報収集 (装置・インタフェース状態表示，運用メッセージ，ログ，統計情報) • NTP	解説書 Vol.2　13. RADIUS/TACACS+ 解説書 Vol.2　14. 運用機能

（凡例）- : 該当なし

2 装置構成

この章では，本装置の各モデルの構成要素や外観など，各装置本体について説明します。

2.1　本装置のモデル

SB-7800S には次に示すモデルがあります。

- SB-7804S
- SB-7808S
- SB-7816S

SB-5400S には次に示すモデルがあります。

- SB-5402S
- SB-5404S

これらのモデルは統一したアーキテクチャで設計しています。本装置のモデルの種類を次の表に示します。

表 2-1　本装置のモデルの種類

モデル	用途
SB-7804S，SB-7808S，SB-7816S	企業向け大規模構内ネットワーク向けモデル キャリア・ISP 向け小容量モデル
SB-5402S，SB-5404S	企業向け中規模／大規模構内ネットワーク向けモデル

2.1.1　収容インタフェース数

本装置が収容できる最大インタフェース数を次の表に示します。表中の数値は単一メディアだけを搭載した場合です。使用する機能や搭載するメディアの組み合わせによって収容回線数の条件が決まります。

表 2-2　SB-7800S の収容インタフェース数

イーサネット	SB-7804S	SB-7808S	SB-7816S
10GBASE-R	4/8※1	8/16※1	16/32※1
10GBASE-W	4	8	16
1000BASE-X(GBIC)	24	48	96
1000BASE-X(SFP)	48/96※1	96/192※1	192/384※1
10BASE-T/100BASE-TX/1000BASE-T	48/96※1※2	96/192※1※2	192/384※1※2

注※1

PSU 内蔵型高密度ポート NIF によってサポート

注※2

オーバサブスクライブ版 NIF によってサポート

表 2-3　SB-7800S の収容インタフェース数 (POS)

POS	SB-7804S	SB-7808S	SB-7816S
OC-192c/STM-64 POS	4	8	16
OC-48c/STM-16 POS	16	32	64

表 2-4　SB-5400S の収容インタフェース数

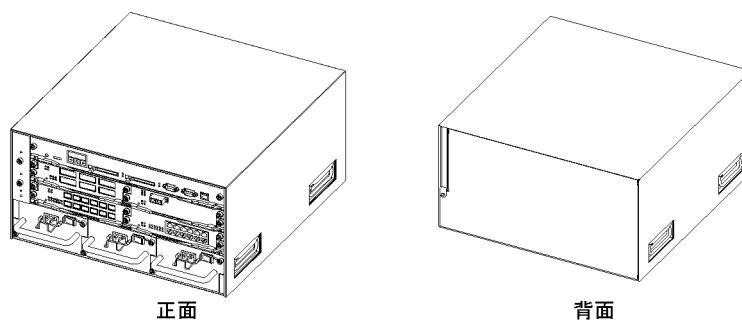
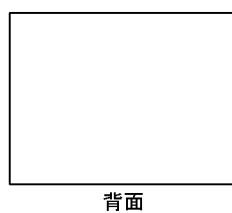
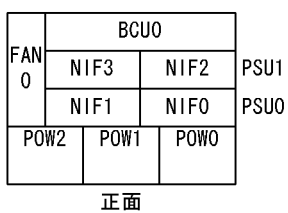
イーサネット	SB-5402S	SB-5404S
1000BASE-X(GBIC)	12	24
1000BASE-X(SFP)	64※	128※
10BASE-T/100BASE-TX	96	192
10BASE-T/100BASE-TX/1000BASE-T	96※	192※

注※　オーバサブスクライブ版 NIF によってサポート

2.1.2　装置の外観

(1)　SB-7804S-AC

SB-7804S-AC の外観を次の図に示します。SB-7804S-AC は，SB-7804S モデルのうち装置の奥行きを抑え，AC100V/AC200V 電源を使用するタイプです。

図 2-1　SB-7804S-AC の外観

●ボードの搭載位置

(2)　SB-7804S-DC

SB-7804S-DC の外観を次の図に示します。SB-7804S-DC は，SB-7804S モデルのうち装置の高さを抑え，DC-48V 電源を使用するタイプです。

図 2-2　SB-7804S-DC の外観

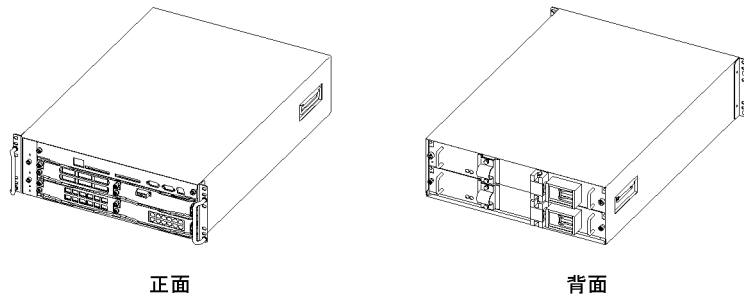
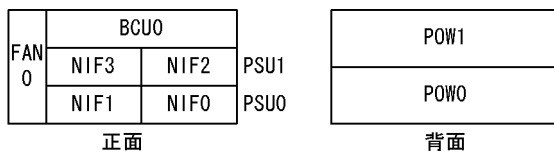
正面

背面

●ボードの搭載位置

FAN 0	BCU0		
	NIF3	NIF2	PSU1
	NIF1	NIF0	PSU0

正面

背面

（3） SB-7808S-AC

SB-7808S-AC の外観を次の図に示します。SB-7808S-AC は，SB-7808S モデルのうち装置の奥行きを抑え，AC100V/AC200V 電源を使用するタイプです。

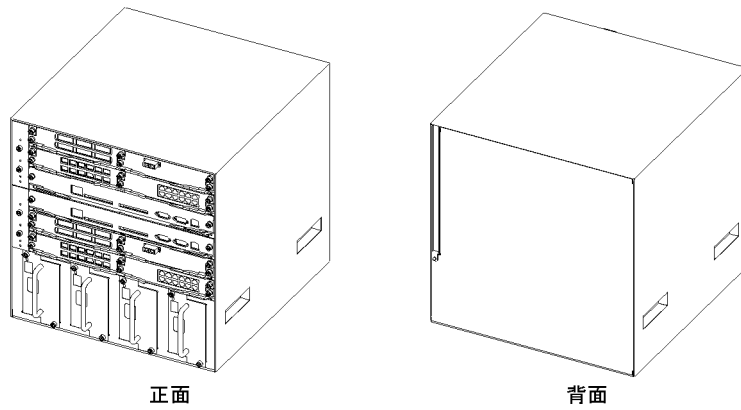
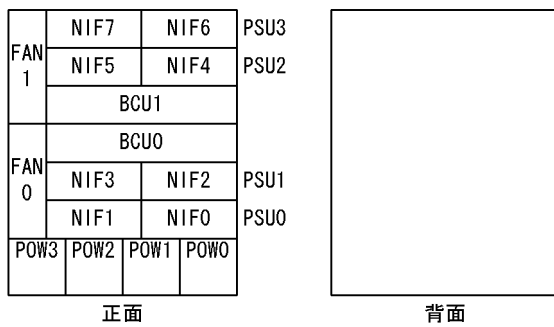
図 2-3　SB-7808S-AC の外観

正面

背面

●ボードの搭載位置

正面

背面

（4） SB-7808S-DC

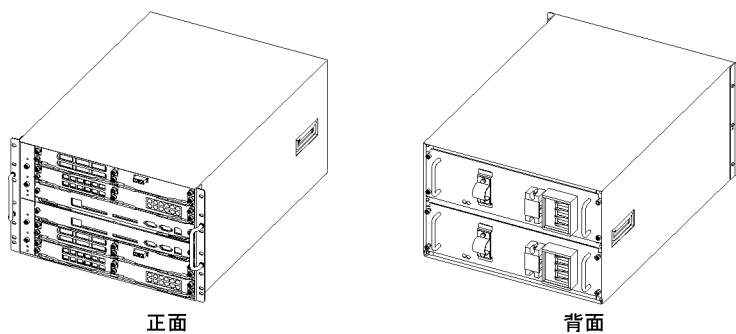
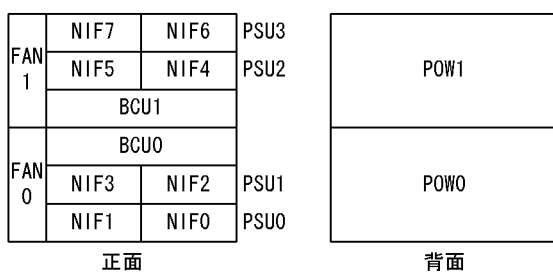
SB-7808S-DC の外観を次の図に示します。SB-7808S-DC は，SB-7808S モデルのうち装置の高さを抑え，DC-48V 電源を使用するタイプです。

図 2-4　SB-7808S-DC の外観

●ボードの搭載位置

FAN 1	NIF7	NIF6	PSU3
	NIF5	NIF4	PSU2
	BCU1		
FAN 0	BCU0		
	NIF3	NIF2	PSU1
	NIF1	NIF0	PSU0

正面

背面

（5） SB-7816S-AC

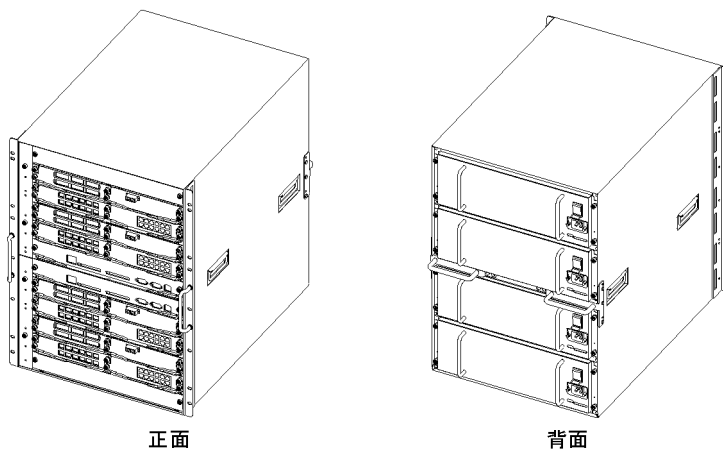
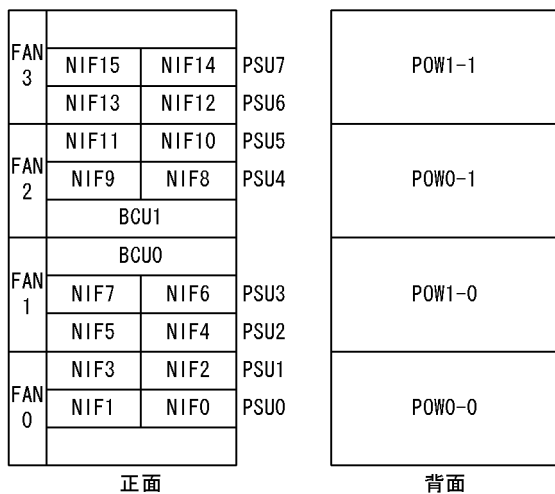
SB-7816S-AC の外観を次の図に示します。SB-7816S-AC は，SB-7816S モデルのうち，AC200V 電源を使用するタイプです。

図 2-5　SB-7816S-AC の外観

●ボードの搭載位置

FAN			
FAN 3			
	NIF15	NIF14	PSU7
	NIF13	NIF12	PSU6
FAN 2	NIF11	NIF10	PSU5
	NIF9	NIF8	PSU4
	BCU1		
FAN 1	BCU0		
	NIF7	NIF6	PSU3
	NIF5	NIF4	PSU2
FAN 0	NIF3	NIF2	PSU1
	NIF1	NIF0	PSU0

正面

背面

（6） SB-7816S-DC

SB-7816S-DC の外観を次の図に示します。SB-7816S-DC は，SB-7816S モデルのうち，DC-48V 電源を使用するタイプです。

図 2-6　SB-7816S-DC の外観

正面

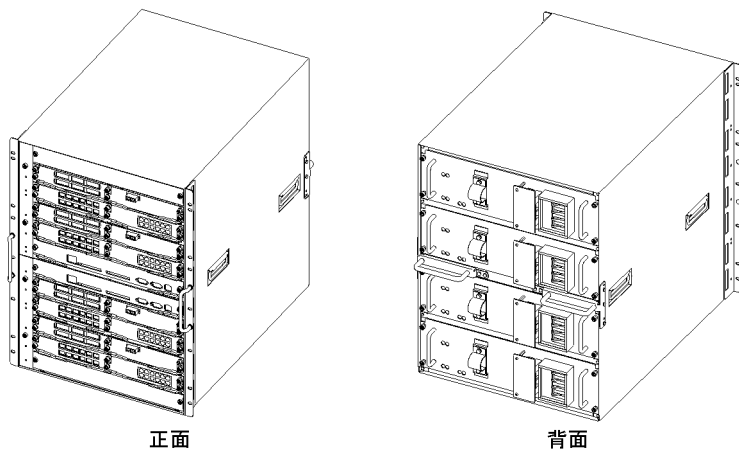
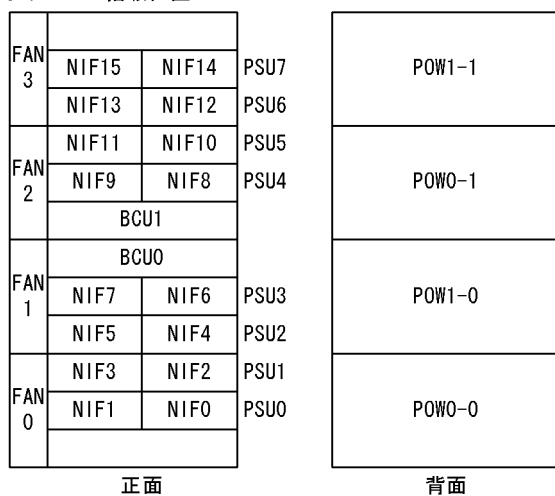
背面

●ボードの搭載位置

FAN			
FAN 3			
	NIF15	NIF14	PSU7
	NIF13	NIF12	PSU6
FAN 2	NIF11	NIF10	PSU5
	NIF9	NIF8	PSU4
	BCU1		
FAN 1	BCU0		
	NIF7	NIF6	PSU3
	NIF5	NIF4	PSU2
FAN 0	NIF3	NIF2	PSU1
	NIF1	NIF0	PSU0

正面

背面
POW1-1
POW0-1
POW1-0
POW0-0

背面

（7） SB-5402S-AC

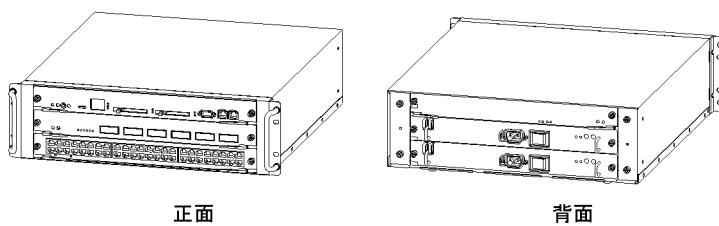
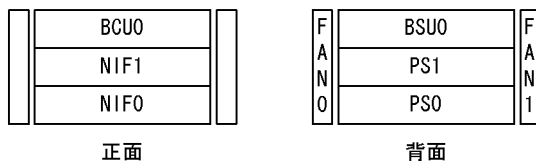
SB-5402S-AC の外観を次の図に示します。

図 2-7　SB-5402S-AC の外観

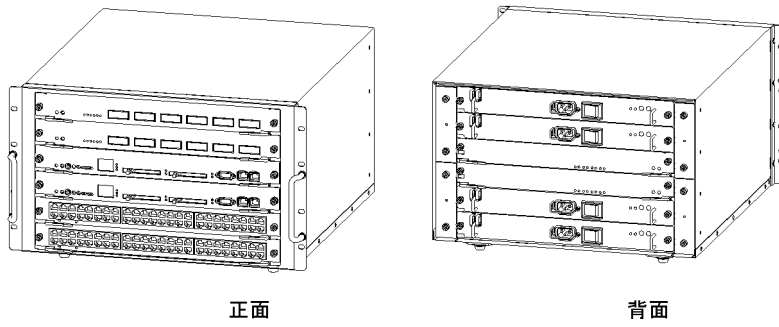
正面　　　　　　　　背面

●ボードの搭載位置

正面

背面

（8） SB-5404S-AC

SB-5404S-AC の外観を次の図に示します。

図 2-8　SB-5404S-AC の外観

●ボードの搭載位置

正面
NIF3
NIF2
BCU1
BCU0
NIF1
NIF0

背面		
FAN2	PS3	FAN3
	PS2	
	BSU1	
FAN0	BSU0	FAN1
	PS1	
	PS0	

2.2 装置の構成要素

本装置を構成している構成要素を，ハードウェアおよびソフトウェアに分けて説明します。

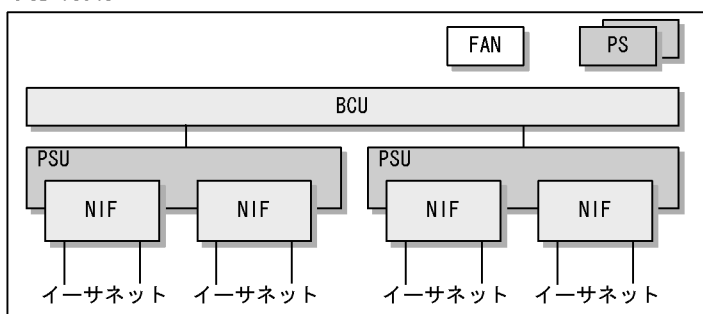
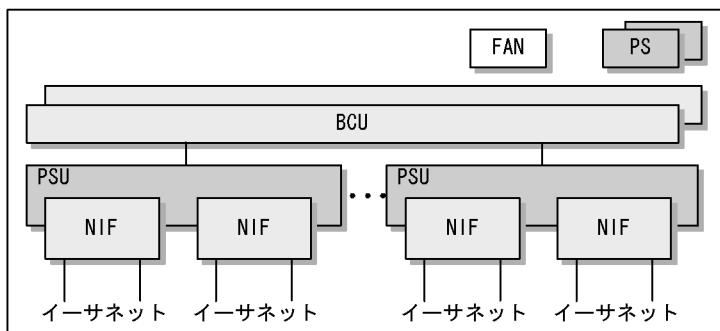
2.2.1 SB-7800S ハードウェアの構成要素【SB-7800S】

ハードウェアの構成要素について説明します。

(1) 各装置の概略

各装置の概略を次の図に示します。

図 2-9 各装置の概略

●SB-7804S

●SB-7808S，SB-7816S

(2) シャーシ

本装置のモデルにそれぞれ対応したシャーシで，ファンなどが含まれています。各シャーシの構成要素と搭載できる最大モジュール数を次の表に示します。

表 2-5 各シャーシの構成要素と搭載できる最大モジュール数

構成要素	シャーシ					
	SB-7804S-AC	SB-7804S-DC	SB-7808S-AC	SB-7808S-DC	SB-7816S-AC	SB-7816S-DC
BCU	1	1	2※1	2※1	2※1	2※1
PSU	2	2	4	4	8	8
NIF	4	4	8	8	16	16
PS(AC100V/AC200V)	3※2	0	4※2	0	0	0

構成要素	シャーシ					
	SB-7804S-AC	SB-7804S-DC	SB-7808S-AC	SB-7808S-DC	SB-7816S-AC	SB-7816S-DC
PS(AC200V)	0	0	0	0	4※1	0
PS(DC-48V)	0	2※1	0	2※1	0	4※1

注※1　2 式搭載して二重化できます (SB-7816S-AC および SB-7816S-DC の電源ユニットは 2 個 / 式となっています)。

注※2　電源ユニットの搭載数は，PSU 内蔵型高密度ポート NIF を使用する場合と使用しない場合とで異なります。

- SB-7804S-AC で PSU 内蔵型高密度ポート NIF を使用しない場合
  電源部を冗長化しないときは電源を 1 個搭載します。電源部を冗長化するときは 2 個または 3 個搭載します。
- SB-7804S-AC で PSU 内蔵型高密度ポート NIF を使用する場合
  電源部を冗長化しないときは電源を 2 個搭載します。電源部を冗長化するときは 3 個搭載します。
- SB-7808S-AC で PSU 内蔵型高密度ポート NIF を使用しない場合
  電源部を冗長化しないときは電源を 2 個搭載します。電源部を冗長化するときは 4 個搭載します。
- SB-7808S-AC で PSU 内蔵型高密度ポート NIF を使用する場合
  電源部を冗長化しないときは電源を 3 個搭載します。電源部を冗長化するときは 4 個搭載します。

(3) 基本制御モジュール (BCU)

BCU(Basic management Control module) は**ルーティングマネージャ** (RM)，**マルチレイヤコントロールプロセッサ** (CP)，および**クロスバースイッチ** (CSW) から構成されます。SB-7808S および SB-7816S では BCU を 2 式搭載することで，基本制御モジュールを二重化できます。各装置の BCU 型名略称と構成を次の表に示します。

表 2-6　各装置の BCU 型名略称と構成

シャーシ	BCU 型名略称	構成
SB-7804S	BCU-SH8MS	• SB-7804S 用 BCU ボード
SB-7808S	BCU-SM8MS	• SB-7808S 用 BCU ボード
	BCU-SM8MS2※1	• SB-7808S 用 BCU ボード 性能向上版
SB-7816S	BCU-SL8MS	• SB-7816S 用 BCU ボード
	BCU-SL8MS2※1	• SB-7816S 用 BCU ボード 性能向上版

注※1　このタイプの BCU を BCU-2 と呼びます。

BCU には，二つの RS232C コンソールポートと，二つのコンパクトフラッシュカード (MC) スロットと，一つの 10BASE-T/100BASE-TX ポートがあります。

(a) ルーティングマネージャ (RM)

RM(Routing Manager) は装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティングテーブルを作成・更新し，ルーティングテーブルを PSU に配布します。

BCU-SH8MS，BCU-SM8MS，BCU-SM8MS2，BCU-SL8MS，および BCU-SL8MS2 の RM には PentiumIII(850MHz) プロセッサと四つのメインメモリー (MS) スロットがあります。メインメモリーの容量は 256MB(MS256) なので，最大で 1GB のメモリを実装できます。

(b) マルチレイヤコントロールプロセッサ (CP)

CP(Multi layer Control Processor) は，IP パケットのソフトウェア中継処理やネットワークインタフェースのプロトコル処理を行います。

(c) クロスバースイッチ (CSW)

CSW(Crossbar Switch) は，RM と PSU，PSU と PSU 間のパケット送受信を，独立して高速に行います。

(4) パケットスイッチングモジュール (PSU)

PSU(Packet Switching Module) に**ルーティング・QoS テーブル検索エンジン** (Routing/QoS-table lookup ASIC) が搭載されています。本装置はハードウェアでルーティングテーブル，フィルタリング・テーブルおよび QoS(Quality of Service) テーブルを検索し，パケットの送受信を行います。これによって高速な処理を実現しています。

また，PSU の代わりに，PSU 内蔵型高密度ポート NIF を使用できます。

PSU の概要を次の表に示します。

表 2-7　PSU の概要

PSU の種類	機能
PSU-1，PSU-12	パケットスイッチングプロセッサ 1，パケットスイッチングプロセッサ 12 • L3 スイッチ機能 • テーブルサイズ基本
PSU-2，PSU-22	パケットスイッチングプロセッサ 2，パケットスイッチングプロセッサ 22 • L3 スイッチ機能 • テーブルサイズ拡張
PSU-33	パケットスイッチングプロセッサ 33 • L3 スイッチ機能 • テーブルサイズ：インターネットルート接続
PSU-43	パケットスイッチングプロセッサ 43 • L3 スイッチ機能 • テーブルサイズ基本 • MAC VLAN 機能

(5) ネットワークインタフェースモジュール (NIF)

NIF(Network Interface board) は各種メディア対応のインタフェース制御部で，複数の種類があり，物理レイヤの処理を行います。

NIF には，高密度実装によって多ポートの収容を可能にした高密度ポート NIF と，通常の NIF(標準ポート NIF) があります。さらに，高密度ポート NIF は PSU を内蔵する NIF(PSU 内蔵型高密度ポート NIF) と PSU を内蔵しない NIF(PSU 分離型高密度ポート NIF) に分かれます。NIF の種別を「図 2-10　NIF の種別」に示します。

また，標準ポート NIF は PSU 当たり最大 2 枚搭載可能，PSU 分離型高密度ポート NIF は PSU 当たり最大 1 枚搭載可能となっています。本装置の PSU は標準で標準ポート NIF を搭載できる構造になっています。PSU 分離型高密度ポート NIF を搭載する場合には，PSU のガイドを外して搭載します。NIF の搭載方法を「図 2-11　標準ポート NIF の搭載方法」～「図 2-13　PSU 内蔵型高密度ポート NIF の搭載方法」に示します。

図 2-10　NIF の種別

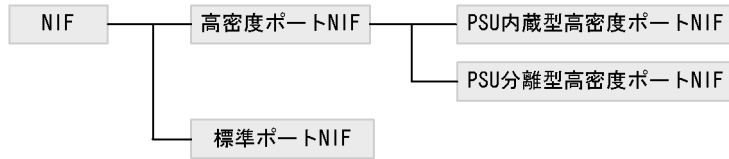



図 2-11　標準ポート NIF の搭載方法

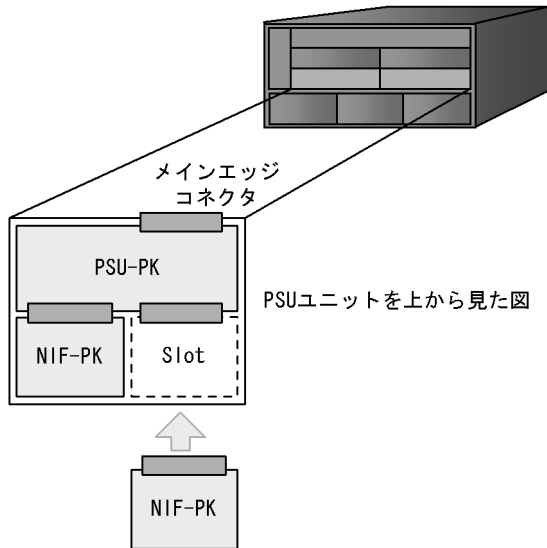



図 2-12　PSU 分離型高密度ポート NIF の搭載方法

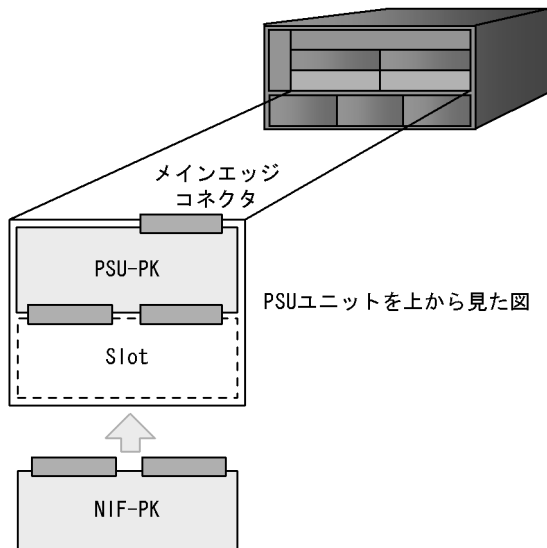



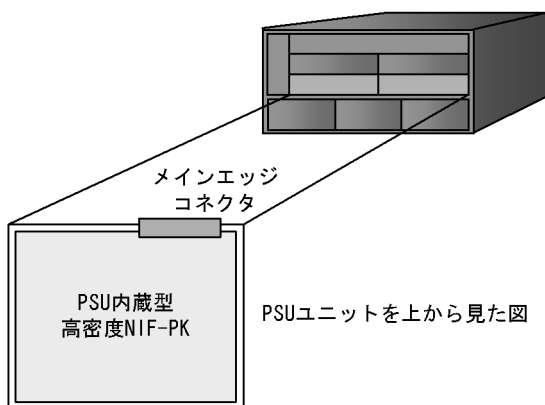
図 2-13　PSU 内蔵型高密度ポート NIF の搭載方法

本装置に搭載できる NIF の種類を次の表に示します。

表 2-8　ネットワークインタフェースモジュール (NIF) の種類

分類	NIF 略称	インタフェース	NIF 種別
イーサネット	NE1GSHP-4S	1000BASE-X，SFP，4 回線，階層化シェーパ機能付き (1023 ユーザ× 4QoS/ ポート)	標準
	NE1GSHP-8S	1000BASE-X，SFP，8 回線，階層化シェーパ機能付き (1023 ユーザ× 4QoS/ ポート)	標準
	NE10G-1ER	10GBASE-ER (2m ～ 40km)，1 回線	標準
	NE10G-1RX	10GBASE-R，XFP，1 回線	標準
	NE10G-1LW	10GBASE-LW (2m ～ 10km)，1 回線	標準
	NE10G-1EW	10GBASE-EW (2m ～ 40km)，1 回線	標準
	NE1G-12SA	1000BASE-X，SFP，12 回線	標準
	NE1G-12TA	10BASE-T/100BASE-TX/1000BASE-T，12 回線	標準
	NE1G-6GA	1000BASE-X，GBIC，6 回線	標準
	NE1G-48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線	高密度 (PSU 分離型)
	S12-1G48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線，PSU-12 内蔵	高密度 (PSU 内蔵型)
	S12-1G48S	1000BASE-X，SFP，48 回線，PSU-12 内蔵	高密度 (PSU 内蔵型)
	S22-10G4RX	10GBASE-R，XFP，4 回線，PSU-22 内蔵	高密度 (PSU 内蔵型)
	S33-10G4RX	10GBASE-R，XFP，4 回線，PSU-33 内蔵	高密度 (PSU 内蔵型)
	NEMX-12	10BASE-T/100BASE-TX/1000BASE-T，8 回線 +1000BASE-X, SFP，4 回線	標準
POS	NP192-1S	OC-192c/STM-64 POS(2km)，1 回線，G.652 シングルモード	標準
	NP192-1S4	OC-192c/STM-64 POS(40km)，1 回線，G.652 シングルモード	標準

分類	NIF 略称	インタフェース	NIF 種別
	NP48-4S	OC-48c/STM-16 POS，SFP，4 回線，シングルモード	標準

ネットワークインタフェースモジュールに搭載して使用する光モジュール（GBIC，SFP，XFP）を合わせてトランシーバと呼びます。

本装置に搭載できるトランシーバの種類を次の表に示します。

表 2-9　トランシーバの種類

分類	トランシーバ種別	トランシーバ略称	機能	上位ネットワークインタフェースモジュール
イーサネット	GBIC	GBIC-SX	1000BASE-SX 用 GBIC	NE1G-6GA
		GBIC-LX	1000BASE-LX 用 GBIC	
		GBIC-LH	1000BASE-LH 用 GBIC	
	SFP	SFP-SX	1000BASE-SX 用 SFP	NE1G-12SA NE1GSHP-4S NE1GSHP-8S S12-1G48S NEMX-12
		SFP-LX	1000BASE-LX 用 SFP	
		SFP-LH	1000BASE-LH 用 SFP	
POS		SFP-P48SR	OC-48c/STM-16 POS 用 SFP 2km	NP48-4S
		SFP-P48LR	OC-48c/STM-16 POS 用 SFP 40km	
イーサネット	XFP	XFP-SR	10GBASE-SR 用 XFP	NE10G-1RX S22-10G4RX S33-10G4RX
		XFP-LR	10GBASE-LR 用 XFP	
		XFP-ER	10GBASE-ER 用 XFP	

(6) 電源ユニット (PS)

PS(Power Supply) は，外部供給電源から装置内で使用する各種直流電源（5V，3.3V ほか）を生成します。各装置の PS 型名略称と構成を次の表に示します。

表 2-10　各装置の PS 型名略称と構成

シャーシ	PS 型名略称	構成
SB-7804S-AC SB-7808S-AC	POW-HMACE	SB-7804S-AC，SB-7808S-AC 用 PS(AC100V/AC200V(50/60Hz))
SB-7816S-AC	POW-MSACE	SB-7816S-AC 用 PS(AC200V(50/60Hz))
	POW-MSACE2	SB-7816S-AC 用 PS(AC200V(50/60Hz)) 性能強化版
SB-7804S-DC	POW-HSDCE	SB-7804S-DC 用 PS(DC-48V)
	POW-HSDCE2	SB-7804S-DC 用 PS(DC-48V) 性能強化版
SB-7808S-DC SB-7816S-DC	POW-MSDCE	SB-7808S-DC，SB-7816S-DC 用 PS(DC-48V)
	POW-MSDCE2	SB-7808S-DC，SB-7816S-DC 用 PS(DC-48V) 性能強化版

注　SB-7816S-AC および SB-7816S-DC の電源ユニットは 2 個 / 式となっています。

SB-7804S-DC，SB-7808S-DC，SB-7816S-AC，SB-7816S-DC では同一種の電源を 2 式搭載して電源部を二重化できます。また，本装置は PS への外部供給電源をそれぞれ独立に接続できるので，外部電源系統を 2 系統化にできます。外部電源系統を 2 系統化にすれば，一方の電源系統が電源工事などで停電した場合でも本装置を継続して使用できます。ただし，異なる配電盤から電源を供給する必要があります。

SB-7804S-AC，SB-7808S-AC では電源を 1 個追加で搭載することにより電源部を冗長化できます。また，PSU 内蔵型高密度ポート NIF を使用していない場合には，外部電源系統を 2 系統化することができます。

（7） メインメモリー (MS)

MS(Main Storage) には 256MB の MS256 があります。

（8） コンパクトフラッシュカード (MC)

MC(Memory Card) は 256MB(MC256/MC256A1) のコンパクトフラッシュカードです。ソフトウェア，コンフィグレーション，ログ情報格納などに使用します。ファイルのバックアップのためコンパクトフラッシュカードは BCU ごとに 2 枚搭載することをお勧めします。MC256/MC256A1 は，BCU-SH8MS，BCU-SM8MS，BCU-SM8MS2，BCU-SL8MS，および BCU-SL8MS2 の場合に使用します。

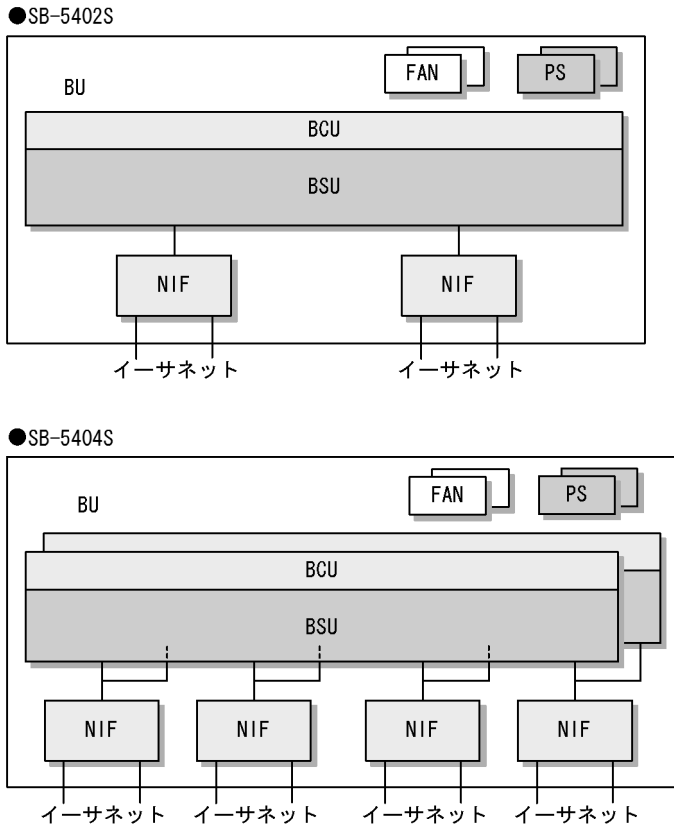
なお，SB-5400S の MC とは形式が異なります。

2.2.2　SB-5400S ハードウェアの構成要素【SB-5400S】

ハードウェアの構成要素について説明します。

（1） 各装置の概略

各装置の概略を次の図に示します。

図 2-14　各装置の概略

（2） シャーシ

本装置のモデルにそれぞれ対応したシャーシで，ファンなどが含まれています。各シャーシの構成要素と搭載できる最大モジュール数を次の表に示します。

表 2-11　各シャーシの構成要素と搭載できる最大モジュール数

構成要素	シャーシ	
	SB-5402S-AC	SB-5404S-AC
BCU	1	2
BSU	1	2
NIF	2	4
PS(AC100V/AC200V)	2※	4※
PS(DC-48V)	2※	4※

注※　2 式搭載して二重化できます (SB-5404S-AC の電源ユニットは 2 個 / 式となっています)。

(3) 基本制御モジュール (BU)

BU(Basic control Unit) は，基本制御モジュール (BCU) および基本スイッチングモジュール (BSU) から構成されます。SB-5404S-AC では，基本制御モジュールを 2 式搭載することで二重化できます。

(4) 基本制御モジュール (BCU)

BCU(Basic management Control module) はルーティングマネージャ (RM)，マルチレイヤコントロールプロセッサ (CP) から構成されます。各装置の BCU 型名略称と構成を次の表に示します。

表 2-12　各装置の BCU 型名略称と構成

シャーシ	BCU 型名略称	構成
SB-5402S-AC	BCU-C5MS	• SB-5402S-AC 用 BCU ボード
SB-5404S-AC	BCU-S5MS	• SB-5404S-AC 用 BCU ボード

BCU には，一つの RS232C コンソールポートと，二つのコンパクトフラッシュカード (MC) スロットと，二つの 10BASE-T/100BASE-TX ポートがあります。

(a) ルーティングマネージャ (RM)

RM(Routing Manager) は装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティングテーブルを作成・更新し，ルーティングテーブルを BSU に配布します。

RM には四つのメインメモリー (MS) スロットがあります。メインメモリーの容量は 256MB(MS256) なので，最大で 1GB のメモリを実装できます。

(b) マルチレイヤコントロールプロセッサ (CP)

CP(Multi layer Control Processor) は，IP パケットのソフトウェア中継処理やネットワークインタフェースのプロトコル処理を行います。

(5) 基本スイッチングモジュール (BSU)

BSU(Basic packet Switching module) にはルーティング・QoS テーブル検索エンジン (Routing/QoS-table lookup ASIC) およびパケット送信エンジン (Packet forwarding ASIC) が搭載されています。本装置はハードウェアでルーティングテーブル，フィルタリング・テーブルおよび QoS(Quality of Service) テーブルを検索し，パケットの送受信を行います。これによって高速な処理を実現しています。

各装置の BSU 型名略称と構成を次の表に示します。

表 2-13　各装置の BSU 型名略称と構成

シャーシ	BSU 型名略称	構成
SB-5402S-AC	BSU-C1，BSU-C2	SB-5402S-AC 用 BSU ボード
SB-5404S-AC	BSU-S1，BSU-S2	SB-5404S-AC 用 BSU ボード

(6) ネットワークインタフェースモジュール (NIF)

NIF(Network Interface board) は各種メディア対応のインタフェース制御部で，複数の種類があり，物理レイヤの処理を行います。

本装置に搭載できる NIF の種類を次の表に示します。

表 2-14　ネットワークインタフェースモジュール (NIF) の種類

分類	NIF 略称	インタフェース
イーサネット	NF1G-6G	1000BASE-X，GBIC，6 回線
	NF100-48TA	10BASE-T/100BASE-TX，48 回線，マイナーチェンジ版
	NF1G-48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線
	NF1G-32S	1000BASE-X，SFP，32 回線
	NFMX-44	10BASE-T/100BASE-TX/1000BASE-T，40 回線 + 1000BASE-X，SFP，4 回線
	NFMX-34	10BASE-T/100BASE-TX/1000BASE-T，32 回線 + 10BASE-T/100BASE-TX/1000BASE-T，あるいは 1000BASE-X，SFP，選択型 2 回線，レガシーシェーパ機能付き

ネットワークインタフェースモジュールに搭載して使用する光モジュール（GBIC，SFP，XFP）を合わせてトランシーバと呼びます。ただし，SB-5400S では XFP は使用しません。

本装置に搭載できるトランシーバの種類を次の表に示します。

表 2-15　トランシーバの種類

分類	トランシーバ種別	トランシーバ略称	機能	上位ネットワークインタフェースモジュール
イーサネット	GBIC	GBIC-SX	1000BASE-SX 用 GBIC	NF1G-6G
		GBIC-LX	1000BASE-LX 用 GBIC	
		GBIC-LH	1000BASE-LH 用 GBIC	
	SFP	SFP-SX	1000BASE-SX 用 SFP	NF1G-32S NFMX-44 NFMX-34
		SFP-LX	1000BASE-LX 用 SFP	
		SFP-LH	1000BASE-LH 用 SFP	

(7) 電源ユニット (PS)

PS(Power Supply) は，外部供給電源から装置内で使用する各種直流電源（5V，3.3V ほか）を生成します。各装置の PS 型名略称と構成を次の表に示します。

表 2-16　各装置の PS 型名略称と構成

シャーシ	PS 型名略称	構成
SB-5402S-AC SB-5404S-AC	PS-CAC	SB-5402S-AC，SB-5404S-AC 用 PS(AC100V/AC200V(50/60Hz))
	PS-CDC	SB-5402S-AC，SB-5404S-AC 用 PS(DC-48V)

注　SB-5404S-AC の電源ユニットは 2 個 / 式となっています。

本装置では同一種の電源を 2 式搭載して電源部を冗長化できます。また，本装置は PS への外部供給電源をそれぞれ独立に接続できるので，外部電源系統を 2 系統化にできます。外部電源系統を 2 系統化にすれば，一方の電源系統が電源工事などで停電した場合でも本装置を継続して使用できます。ただし，異なる

配電盤から電源を供給する必要があります。

(8) メインメモリー (MS)

MS(Main Storage) には 256MB の MS256 があります。

(9) コンパクトフラッシュカード (MC)

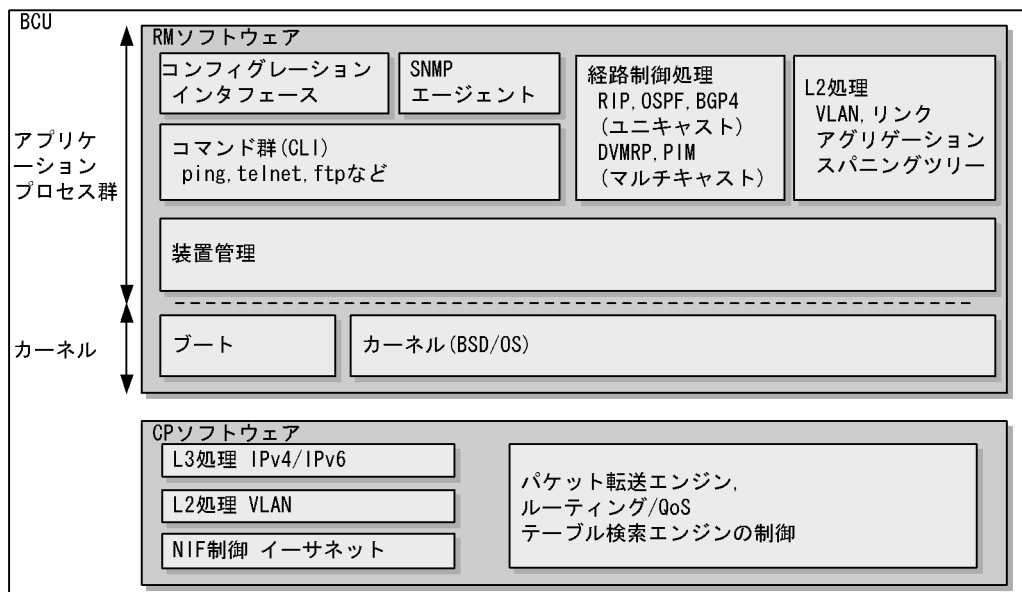
MC(Memory Card) は 256MB のコンパクトフラッシュカードです。ソフトウェア，コンフィグレーション，ログ情報格納などに使用します。ファイルのバックアップのためコンパクトフラッシュカードは BCU ごとに 2 枚搭載することをお勧めします。なお，SB-7800S の MC とは形式が異なります。

2.2.3 ソフトウェア

(1) ソフトウェア構成

ソフトウェアは，RM ソフトウェアと CP ソフトウェアから成ります。RM ソフトウェアは，カーネル部分にインターネットサーバとして安定性の高い BSD/OS の組み込み型版 (embedded BSD/OS) を使用しています。この上に各種プロトコル機能，コマンドなどをアプリケーションプロセスとして実装していますので，機能追加などに柔軟に対応できる構成になっています。一方，CP ソフトウェアは，IP パケットのソフトウェア中継処理およびネットワークインタフェースのプロトコル処理を行います。

ソフトウェア構成を次の図に示します。

図 2-15 ソフトウェア構成

(2) ソフトウェア・オプションライセンス

本装置のソフトウェアは，基本ソフトとオプションライセンスとに分けて提供します。基本ソフト OS-SW はベースとなるソフトウェアで，IP パケット中継機能や RIP/OSPF※などの基本機能が含まれます。オプションライセンスは，本装置のサポートする主要な拡張機能をオプション形式で提供するライセンスです。お客様のニーズに合わせて必要な機能のオプションライセンスだけを追加してご購入いただくことができます。初期導入後に追加で別のオプションライセンスをご購入いただくこともできます。これによって，初期導入時のコストを抑えることができます。本装置で提供するオプションライセンスの一覧を次の表に示します。

注※

SB-5400S では，利用可能な機能の選択の自由度を増やすために OSPF 機能をオプションライセンス化しています。このため SB-5400S の基本ソフト OS-SW には，OSPF が含まれません。

表 2-17 ソフトウェア・オプションライセンス一覧

オプションライセンス	概要	対応する機能
OP-BGP	BGP 機能を追加するライセンス	BGP4/BGP4+
OP-MLT	IP マルチキャスト機能を追加するライセンス	DVMRP，PIM-DM，PIM-SM/SSM

オプションライセンス	概要	対応する機能
OP-ISIS	IS-IS 機能を追加するライセンス	IS-IS
OP-OSPF	OSPF 機能を追加するライセンス	OSPF，OSPFv3
OP-ADV	先進機能を追加するライセンス	NetFlow Version 9

(a) OP-ADV について

このマニュアルでの「先進機能」とは，標準化や業界の動向が固まっていないため，その動向次第で外部仕様を変更することもある段階の機能のことを指します。対応する機能が今後追加された場合には，そのすべての機能を使用することができます。

対応する機能について標準化や業界の動向が固まった時点で，将来のバージョンアップで基本ソフトウェアに組み込む場合があります。この場合，このオプションライセンスを削除してください。設定の反映には装置の再起動が必要です。削除の方法は「オプションライセンス設定ガイド」を参照してください。

将来，対応する機能が無くなった場合，本装置のソフトウェアから OP-ADV は無くなります。

その後，対応する機能が追加され，該当機能を使用する場合は，このオプションライセンスを有効化してください。

2.3 接続形態

各種インタフェースの接続仕様を次の表に示します。

表 2-18 各種インタフェースの接続仕様【SB-7800S】

物理インタフェース	NIF 略称	ケーブル仕様	最短 (m)	最長 (m)	コネクタ
10BASE-T	NE1G-12TA NE1G-48T S12-1G48T NEMX-12	カテゴリー 3/4/5 4 芯 /8 芯 2 対ストレート	-	100	RJ45
100BASE-TX		カテゴリー 5 8 芯 2 対ストレート	-	100	
1000BASE-T		カテゴリー 5E 8 芯 4 対ストレート	-	100	
1000BASE-SX	NE1GSHP-4S NE1GSHP-8S NE1G-12SA S12-1G48S NEMX-12	マルチモード光ファイバ コア径 / クラッド径＝ 50/125μm 波長＝ 850nm，400MHz 帯	2	500	LC 2 芯
		マルチモード光ファイバ コア径 / クラッド径＝ 62.5/125μm 波長＝ 850nm，200MHz 帯	2	275	
1000BASE-LX		マルチモード光ファイバ※1 コア径 / クラッド径＝ 50/125μm 波長＝ 1300nm，500MHz 帯	2	550	
		マルチモード光ファイバ※1 コア径 / クラッド径＝ 62.5/125μm 波長＝ 1300nm，500MHz 帯	2	550	
		シングルモード光ファイバ コア径 / クラッド径＝ 10/125μm 波長＝ 1310nm	2	5k	
1000BASE-LH		シングルモード光ファイバ コア径 / クラッド径＝ 10/125μm 波長＝ 1550nm	2※2	70k	
		シングルモード光ファイバ コア径 / クラッド径＝ 8/125μm 波長＝ 1550nm	2※2	70k	
1000BASE-SX	NE1G-6GA	マルチモード光ファイバ コア径 / クラッド径＝ 50/125μm 波長＝ 850nm，400MHz 帯	2	500	SC2 芯
		マルチモード光ファイバ コア径 / クラッド径＝ 62.5/125μm 波長＝ 850nm，200MHz 帯	2	275	
1000BASE-LX		マルチモード光ファイバ※1 コア径 / クラッド径＝ 50/125μm 波長＝ 1300nm，500MHz 帯	2	550	
		マルチモード光ファイバ※1 コア径 / クラッド径＝ 62.5/125μm 波長＝ 1300nm，500MHz 帯	2	550	
		シングルモード光ファイバ コア径 / クラッド径＝ 10/125μm 波長＝ 1310nm	2	5k	
1000BASE-LH		シングルモード光ファイバ コア径 / クラッド径＝ 10/125μm 波長＝ 1550nm	2※2	70k	
		シングルモード光ファイバ コア径 / クラッド径＝ 8/125μm 波長＝ 1550nm	2※2	70k	

物理インタフェース	NIF 略称	ケーブル仕様	最短 (m)	最長 (m)	コネクタ
10GBASE-SR	NE10G-1RX S22-10G4RX S33-10G4RX	マルチモード光ファイバ　コア径 / クラッド径＝ 50/125μm　波長＝ 850nm，2000MHz 帯	2	300	LC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 50/125μm　波長＝ 850nm，500MHz 帯	2	82	LC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 50/125μm　波長＝ 850nm，400MHz 帯	2	66	LC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 62.5/125μm　波長＝ 850nm，200MHz 帯	2	33	LC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 62.5/125μm　波長＝ 850nm，160MHz 帯	2	26	LC2 芯
10GBASE-LR		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1310nm	2	10k	LC2 芯
10GBASE-ER		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1550nm	2※2	40k	LC 2 芯
	NE10G-1ER	シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1550nm	2※2	40k	SC 2 芯
10GBASE-LW	NE10G-1LW	シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1310nm	2	10k	SC 2 芯
10GBASE-EW	NE10G-1EW	シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1550nm	2※2	40k	SC 2 芯
OC-192c/STM-64 POS	NP192-1S	G.652 シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1310nm	-	2k	SC 2 芯
	NP192-1S4	G.652 シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1550nm	-	40k	SC 2 芯
OC-48c/STM-16 POS	NP48-4S	シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1310nm	-	2k	LC 2 芯
		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125μm　波長＝ 1310nm	-	40k	LC 2 芯

（凡例）- : 該当なし

注※ 1　1000BASE-LX でマルチモード光ファイバを使用する場合，光ファイバによっては BER（ビット・エラー・レート）が上昇することがあります。このような場合には，モード・コンディショニング・パッチコードを使用することで，問題なく通信できます。

注※ 2　距離が短い場合は光減衰器（アッテネータ）が必要です。

表 2-19　各種インタフェースの接続仕様【SB-5400S】

物理インタフェース	NIF 略称	ケーブル仕様	最短 (m)	最長 (m)	コネクタ
10BASE-T	NF100-48TA NF1G-48T NFMX-44 NFMX-34	カテゴリー 3/4/5　4 芯 /8 芯　2 対ストレート	-	100	RJ45
100BASE-TX		カテゴリー 5　8 芯　2 対ストレート	-	100	
1000BASE-T	NF1G-48T NFMX-44 NFMX-34	カテゴリー 5E　8 芯　4 対ストレート	-	100	
1000BASE-SX	NF1G-32S NFMX-44 NFMX-34	マルチモード光ファイバ　コア径 / クラッド径＝ 50/125 μ m　波長＝ 850nm，400MHz 帯	2	500	LC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 62.5/125 μ m　波長＝ 850nm，200MHz 帯	2	275	
1000BASE-LX		マルチモード光ファイバ※ 1　コア径 / クラッド径＝ 50/125 μ m　波長＝ 1300nm，500MHz 帯	2	550	
		マルチモード光ファイバ※ 1　コア径 / クラッド径＝ 62.5/125 μ m　波長＝ 1300nm，500MHz 帯	2	550	
		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125 μ m　波長＝ 1310nm	2	5k	
1000BASE-LH		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125 μ m　波長＝ 1550nm	2 ※ 2	70k	
		シングルモード光ファイバ　コア径 / クラッド径＝ 8/125 μ m　波長＝ 1550nm	2 ※ 2	70k	
1000BASE-SX	NF1G-6G	マルチモード光ファイバ　コア径 / クラッド径＝ 50/125 μ m　波長＝ 850nm，400MHz 帯	2	500	SC2 芯
		マルチモード光ファイバ　コア径 / クラッド径＝ 62.5/125 μ m　波長＝ 850nm，200MHz 帯	2	275	
1000BASE-LX		マルチモード光ファイバ※ 1　コア径 / クラッド径＝ 50/125 μ m　波長＝ 1300nm，500MHz 帯	2	550	
		マルチモード光ファイバ※ 1　コア径 / クラッド径＝ 62.5/125 μ m　波長＝ 1300nm，500MHz 帯	2	550	
		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125 μ m　波長＝ 1310nm	2	5k	
1000BASE-LH		シングルモード光ファイバ　コア径 / クラッド径＝ 10/125 μ m　波長＝ 1550nm	2 ※ 2	70k	
		シングルモード光ファイバ　コア径 / クラッド径＝ 8/125 μ m　波長＝ 1550nm	2 ※ 2	70k	

（凡例）- : 該当なし

注※ 1　1000BASE-LX でマルチモード光ファイバを使用する場合，光ファイバによっては BER（ビット・エラー・レート）が上昇することがあります。このような場合には，モード・コンディショニング・パッチコードを使用するこ

とで，問題なく通信できます。
注※２　距離が短い場合は光減衰器（アッテネータ）が必要です。

2.4　CSW 動作モード（CSW モード）【SB-7800S】

2.4.1　CSW 動作モードについて

BCU 二重化を実装した装置で，運用系 BCU の CSW（Crossbar Switch）を単独で使用する CSW モード（single モード）と，運用系と待機系の BCU 上の CSW を二つ同時に使用する CSW モード（double または double_fixed モード）を運用コマンドで選択でき，PSU 間の中継性能を変更できます。

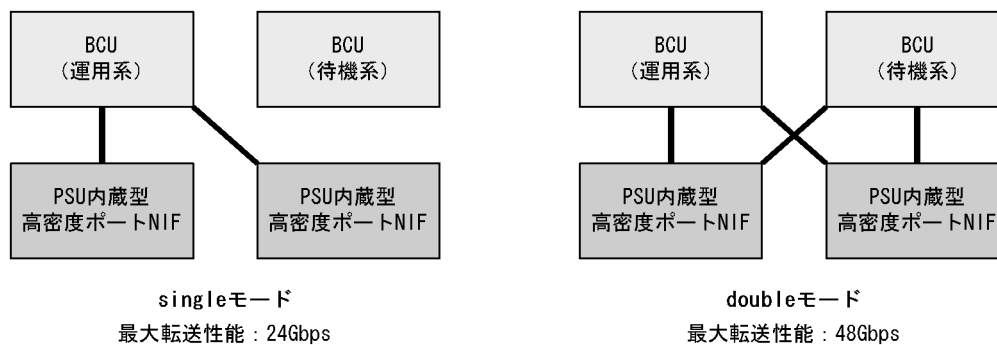
運用コマンドで CSW の動作モードを特に設定しない場合または single モードを選択した場合，PSU 間転送性能は 24Gbps です。CSW モード（double または double_fixed）を選択した場合，CSW を同時に使用できるようになり，PSU 間の中継性能は 48Gbps になります。

PSU 内蔵型高密度ポート NIF を 2 枚以上実装している装置構成の場合，CSW モード（double または double_fixed）を選択すると，PSU 間の中継性能は 48Gbps で運用できるようになります。

ただし，PSU 内蔵型高密度ポート NIF が 1 枚以下の環境や，通常 NIF と PSU の組み合わせの場合，CSW モードを double または double_fixed に設定しても，PSU 当たりの中継性能が 20Gbps 以下となり，設定しても性能が向上することはありません。そのため，このような場合は CSW モード（single モード）での運用を推奨します。

注意事項

この章での中継性能の数値は PSU 間の単一方向の転送性能を表し，PSU 双方向の合計の性能換算では倍の値になります。

図 2-16　CSW 動作モードの動作例

2.4.2　CSW モードの種別と動作概要

CSW モードと動作概要と BCU 冗長化の可否を次の表に示します。

表 2-20　各 CSW モードの動作概要

CSW モード	動作概要	BCU 冗長化
single （初期値）	運用系 BCU の CSW だけを使用するモード。 最大 PSU 間転送性能：24Gbps	可

CSW モード	動作概要	BCU 冗長化
double	運用系と待機系 BCU の CSW を二つ同時に使用するモード。 最大 PSU 間転送性能：48Gbps	可※
double_fixed	運用系と待機系 BCU の CSW を二つ同時に使用するモード。 最大 PSU 間転送性能：48Gbps なお，BCU 障害が発生した場合，通信回線側をダウンします。BCU が回復した場合は，再び通信を再開します。	否

注※　BCU 障害時の PSU 間転送性能は最大 24Gbps となります。

コマンドの入力方法についての詳細は，「運用コマンドレファレンス Vol.2　set mode」を参照してください。

2.4.3 CSW モードの注意事項

各 CSW モードの運用に関する注意事項を次の表に示します。

表 2-21　各 CSW モードの運用に関する注意事項

CSW モード	各モードの注意事項
single	-
double	1. BCU で障害が発生した場合，障害の発生した BCU が復旧するまでの間は，single モード（BCU 1 枚の CSW による中継）に遷移します。そのため，BCU 障害が回復するまでの間は，PSU 間の最大転送能力は 24Gbps になります。 2. 系切替時はいったん新運用系側の BCU だけを利用した CSW モード（single モード）に遷移し，その後待機系の BCU の転送が可能かどうか確認して 48Gbps 転送性能へ遷移するため，2 秒間程度 PSU 間の転送性能が 24Gbps になります。 3. CSW 動作モードを single から double へ変更した場合または系切替をした場合は，24Gbps から 48Gbps 転送への遷移時に 300msec 程度パケット通信が停止します。
double_fixed	1. BCU 二重化を実装していても，BCU 非冗長として動作します。 2. 系切替を抑止しています。 3. BCU で障害が発生した場合は装置障害扱いとなり，PSU 配下の通信を停止します。 4. ソフトウエアをアップデートするときは，いったん，モードを single または double に変更してから実施する必要があります。 5. CSW 動作モードを single から double_fixed に変更した場合，24Gbps から 48Gbps 転送への遷移時に 300msec 程度パケット通信が停止します。

（凡例）- : 特にありません。

3 収容条件

この章では本装置の搭載条件および収容条件について説明します。

3.1 搭載条件

本装置の搭載条件について説明します。

3.1.1 SB-7800S の機器搭載条件【SB-7800S】

モデルごとの機器搭載条件を示します。

（1） 機器最大搭載数

モデルごとの機器最大搭載数を次の表に示します。

表 3-1 機器最大搭載数

機器	SB-7800S モデル					
	SB-7804S-AC	SB-7804S-DC	SB-7808S-AC	SB-7808S-DC	SB-7816S-AC	SB-7816S-DC
電源ユニット (POW)(AC100V/AC200V 対応用)	3※1	0	4※1	0	0	0
電源ユニット (POW)(AC200V 専用)	0	0	0	0	4※2	0
電源ユニット (POW)(DC-48V 用)	0	2※2	0	2※2	0	4※2
基本制御モジュール (BCU)	1	1	2※2	2※2	2※2	2※2
メインメモリー	4/BCU	4/BCU	4/BCU	4/BCU	4/BCU	4/BCU
コンパクトフラッシュカード	2/BCU	2/BCU	2/BCU	2/BCU	2/BCU	2/BCU
パケットスイッチングモジュール (PSU)	2	2	4	4	8	8
ネットワークインタフェースモジュール (NIF)	4	4	8	8	16	16

注※1　電源ユニットの搭載数は，PSU 内蔵型高密度ポート NIF を使用する場合と使用しない場合とで異なります。

- SB-7804S-AC で PSU 内蔵型高密度ポート NIF を使用しない場合
  電源部を冗長化しないときは電源を 1 個搭載します。電源部を冗長化するときは 2 個または 3 個搭載します。
- SB-7804S-AC で PSU 内蔵型高密度ポート NIF を使用する場合
  電源部を冗長化しないときは電源を 2 個搭載します。電源部を冗長化するときは 3 個搭載します。
- SB-7808S-AC で PSU 内蔵型高密度ポート NIF を使用しない場合
  電源部を冗長化しないときは電源を 2 個搭載します。電源部を冗長化するときは 4 個搭載します。
- SB-7808S-AC で PSU 内蔵型高密度ポート NIF を使用する場合
  電源部を冗長化しないときは電源を 3 個搭載します。電源部を冗長化するときは 4 個搭載します。

注※2　2 式搭載して二重化できます (SB-7816S-AC および SB-7816S-DC の電源ユニットは 2 個 / 式となっています)。

（2） PSU 搭載条件

モデルごとの PSU 搭載条件を次の表に示します。

表 3-2　モデルごとの PSU 搭載条件

PSU	SB-7800S モデル		
	SB-7804S	SB-7808S	SB-7816S
PSU-1，PSU-12	○	○	○
PSU-2，PSU-22	○	○	○
PSU-33	○	○	○
PSU-43	○	○	○

(凡例)　○ : 利用できる組み合わせ

(3)　NIF 最大搭載数

(a)　各モデルへの NIF 最大搭載数

各モデルの NIF 最大搭載数を次の表に示します。

表 3-3　各モデルの NIF 最大搭載数

NIF 種別	略称	概略仕様	最大搭載数		
			SB-7800S モデル		
			SB-7804S	SB-7808S	SB-7816S
標準ポート NIF	NE1GSHP-4S	1000BASE-X，SFP，4 回線，階層化シェーパ機能付き (1023 ユーザ× 4QoS/ ポート)	4	8	16
	NE1GSHP-8S	1000BASE-X，SFP，8 回線，階層化シェーパ機能付き (1023 ユーザ× 4QoS/ ポート)	4	8	16
	NE10G-1ER	10GBASE-ER(2m 〜 40km)，1 回線	4	8	16
	NE10G-1RX	10GBASE-R，XFP，1 回線	4	8	16
	NE10G-1LW	10GBASE-LW(2m 〜 10km)，1 回線	4	8	16
	NE10G-1EW	10GBASE-EW(2m 〜 40km)，1 回線	4	8	16
	NP192-1S	OC-192c/STM-64 POS(2km)，1 回線，G.652 シングルモード	4	8	16
	NP192-1S4	OC-192c/STM-64 POS(40km)，1 回線，G.652 シングルモード	4	8	16
	NP48-4S	OC-48c/STM-16 POS，SFP，4 回線，シングルモード	4	8	16
	NE1G-12SA	1000BASE-X，SFP，12 回線	4	8	16
	NE1G-12TA	10BASE-T/100BASE-TX/1000BASE-T，12 回線	4	8	16
	NE1G-6GA	1000BASE-X，GBIC，6 回線	4	8	16
	NEMX-12	10BASE-T/100BASE-TX/1000BASE-T，8 回線 + 1000BASE-X，SFP，4 回線	4	8	16
PSU 分離型高密度ポート NIF	NE1G-48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線	2	4	8
PSU 内蔵型高密度ポート NIF	S12-1G48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線，PSU-12 内蔵	2	4	8

NIF 種別	略称	概略仕様	最大搭載数		
			SB-7800S モデル		
			SB-7804S	SB-7808S	SB-7816S
	S12-1G48S	1000BASE-X，SFP，48 回線，PSU-12 内蔵	2	4	8
	S22-10G4RX	10GBASE-R，XFP，4 回線，PSU-22 内蔵	2	4	8
	S33-10G4RX	10GBASE-R，XFP，4 回線，PSU-33 内蔵	2	4	8

(b) NIF 互換性

各 PSU に対する NIF 種別の互換性を次の表に示します。

表 3-4　各 PSU に対する NIF 種別の互換性

分類	NIF 略称	PSU 種別	
		PSU-1 PSU-2	PSU-12 PSU-22 PSU-33 PSU-43
イーサネット	NE1GSHP-4S	○	○
	NE1GSHP-8S	○	○
	NE10G-1ER	○	○
	NE10G-1RX	○	○
	NE10G-1LW	○	○
	NE10G-1EW	○	○
	NE1G-12SA	○	○
	NE1G-12TA	○	○
	NE1G-6GA	○	○
	NEMX-12	○	○
	NE1G-48T	○	○
POS	NP192-1S	×	○
	NP192-1S4	×	○
	NP48-4S	×	○

（凡例）　○：利用できる組み合わせ　×：利用できない組み合わせ

(c) NIF 搭載方法

本装置の PSU は標準では標準ポート NIF を搭載する構造になっています。高密度ポート NIF を搭載する場合には，NIF を搭載する PSU の標準ポート NIF 搭載用のガイドを外して搭載します。

(4) 電源搭載方法

本装置の電源ユニットは，装置ごとに搭載位置が決まっています。装置ごとの電源ユニットの搭載位置については，「ハードウェア取扱説明書」を参照してください。

(5) 増設メモリ単位と搭載メモリ量

基本制御モジュール BCU，BCU-2 のメモリ増設単位と搭載メモリ量を次の表に示します。

表 3-5 基本制御モジュール (BCU，BCU-2) メモリ増設単位と搭載メモリ量

増設単位	SB-7804S	SB-7808S	SB-7816S
	BCU-SH8MS	BCU-SM8MS BCU-SM8MS2	BCU-SL8MS BCU-SL8MS2
ベース	256MB		
256MB 増設 (256MB × 1)	512MB		
512MB 増設 (256MB × 2)	768MB		
768MB 増設 (256MB × 3)	1024MB		

3.1.2　SB-5400S の機器搭載条件【SB-5400S】

モデルごとの機器搭載条件を示します。

（1）機器最大搭載数

モデルごとの機器最大搭載数を次の表に示します。

表 3-6　機器最大搭載数

機器	SB-5400S モデル	
	SB-5402S	SB-5404S
電源ユニット (PS)(AC100V/AC200V 用)	2※	4※
電源ユニット (PS)(DC-48V 用)	2※	4※
基本制御モジュール (BCU)	1	2※
メインメモリー	4/BCU	4/BCU
コンパクトフラッシュカード	2/BCU	2/BCU
基本スイッチングモジュール (BSU)	1	2※
ネットワークインタフェースモジュール (NIF)	2	4

注※
　2 式搭載して二重化できます (SB-5404S の電源ユニットは 2 個 / 式となっています)。

（2）NIF 最大搭載数

（a）各モデルへの NIF 最大搭載数

各モデルの NIF 最大搭載数を次の表に示します。

表 3-7　各モデルの NIF 最大搭載数

NIF ボードサイズ	略称	概略仕様	最大搭載数	
			SB-5400S モデル	
			SB-5402S	SB-5404S
ダブル	NF1G-6G	1000BASE-X，GBIC，6 回線	2	4
	NF100-48TA	10BASE-T/100BASE-TX，48 回線，マイナーチェンジ版	2	4
	NF1G-48T	10BASE-T/100BASE-TX/1000BASE-T，48 回線	2	4
	NF1G-32S	1000BASE-X，SFP，32 回線	2	4
	NFMX-44	10BASE-T/100BASE-TX/1000BASE-T，40 回線 + 1000BASE-X，SFP，4 回線	2	4
	NFMX-34	10BASE-T/100BASE-TX/1000BASE-T，32 回線 + 10BASE-T/100BASE-TX/1000BASE-T，あるいは 1000BASE-X，SFP，選択型 2 回線，レガシーシェーパ機能付き	2	4

（b）NIF 互換性

各 BSU に対する NIF 種別の互換性を次の表に示します。

表 3-8 各 BSU に対する NIF 種別の互換性

分類	NIF 略称	BSU 種別
		BSU-C1，BSU-C2，BSU-S1，BSU-S2
イーサネット	NF1G-6G	○
	NF100-48TA	○
	NF1G-48T	○
	NF1G-32S	○
	NFMX-44	○
	NFMX-34	○

（凡例） ○：利用できる組み合わせ

（3） 電源搭載方法

本装置の電源ユニットは，装置ごとに搭載位置が決まっています。装置ごとの電源ユニットの搭載位置については，「ハードウェア取扱説明書」を参照してください。

（4） 増設メモリ単位と搭載メモリ量

基本制御モジュール (BCU) メモリ増設単位と搭載メモリ量を次の表に示します。

表 3-9 基本制御モジュール (BCU) メモリ増設単位と搭載メモリ量

増設単位	SB-5402S-AC	SB-5404S-AC
	BCU-C5MS	BCU-S5MS
ベース	256MB	
256MB 増設 (256MB × 1)	512MB	
512MB 増設 (256MB × 2)	768MB	
768MB 増設 (256MB × 3)	1024MB	

3.2　収容条件

3.2.1　SB-7800S の収容条件【SB-7800S】

以下に示す条件をすべて満たすようにご使用ください。

（1） PSU の最大テーブルエントリ数

PSU は次に示すテーブルを保有します。PSU-1，PSU-12 および PSU-43 と PSU-2 および PSU-22 との違いは，FDB のテーブルエントリ数です。PSU-2 および PSU-22 は PSU-1，PSU-12 および PSU-43 に比べ 2 倍の FDB のテーブルエントリを保有します。PSU-33 は，BGP フルルートに対応します。

- FDB
- IPv4 ユニキャスト経路 (アクティブ経路)
- IPv4 マルチキャスト経路
- ARP
- IPv6 ユニキャスト経路 (アクティブ経路)
- IPv6 マルチキャスト経路
- NDP

装置としての最大テーブルエントリ数は，「(9) FDB」と「(13) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」以降で示す値と PSU の最大テーブルエントリ数の小さい方の値となります。また，同時に使用できるエントリ数も，「(9) FDB」と「(13) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」以降で示す値と PSU 最大テーブルエントリ数の小さい方の値となります。

ソフトウェアのオプションライセンスとは，独立に収容条件を定めているため，必要なオプションライセンスを購入してください。例えば，IPv4/IPv6 ユニキャスト経路を最大値まで使用する場合は，**【OP-BGP】**が必要です。

本装置では，利用形態に合わせ，各テーブルのエントリ数の配分パターンを用意しています。PSU-1，PSU-12 および PSU-43，PSU-2 および PSU-22，PSU-33 の配分パターンを次の表に示します。配分パターンはコンフィグレーションによって変更できます。PSU-1，PSU-12 および PSU-43 の初期時のパターンは「l3switch-11」，PSU-2 および PSU-22 の初期時のパターンは「l3switch-21」，PSU-33 の初期時のパターンは「l3switch-31」です。

なお，表中の「k」の単位は 1,024 です。例えば，パターン名 l3switch-11 の FDB ＝ 64k は，64 × 1,024 ＝ 65,536 であることを表します。

表 3-10　PSU-1，PSU-12，PSU-2，PSU-22，PSU-33，PSU-43 で共通のテーブルエントリの配分パターン

想定する利用形態		パターン名			
		l3switch-11	l3switch-12	l2switch-11 ※ 2	l2switch-12
		企業向け L3-SW IP マルチキャストなし	企業向け L3-SW IP マルチキャストあり	L2 キャリア FDB 最大	L2 キャリア
L2	FDB	65,536 (64k)	49,152 (48k)	131,072 (128k)	114,688 (112k)

想定する利用形態		パターン名			
		l3switch-11	l3switch-12	l2switch-11 ※2	l2switch-12
		企業向け L3-SW IP マルチキャストなし	企業向け L3-SW IP マルチキャストあり	L2 キャリア FDB 最大	L2 キャリア
IPv4	ユニキャスト経路※1	65,536 (64k)	65,536 (64k)	-	16,384 (16k)
	マルチキャスト経路	-	8,192 (8k)	-	-
	ARP	32,768 (32k)	32,768 (32k)	-	8,192 (8k)
IPv6	ユニキャスト経路※1	16,384 (16k)	16,384 (16k)	-	-
	マルチキャスト経路	-	8,192 (8k)	-	-
	NDP	8,192 (8k)	8,192 (8k)	-	-

(凡例) -:エントリなし

注※1

アクティブ経路

注※2

SNMP や telnet などで本装置を管理する場合には RM イーサネット経由するリモート端末またはコンソール端末を使用することを想定しています。

表 3-11 PSU-2，PSU-22，PSU-33 で共通のテーブルエントリの配分パターン

想定する利用形態		パターン名			
		l3switch-21	l3switch-22	l2switch-21 ※2	l2switch-22
		企業向け L3-SW IP マルチキャストなし	企業向け L3-SW IP マルチキャストあり	L2 キャリア FDB 最大	L2 キャリア
L2	FDB	131,072 (128k)	98,304 (96k)	262,144 (256k)	229,376 (224k)
IPv4	ユニキャスト経路※1	65,536 (64k)	65,536 (64k)	-	16,384 (16k)
	マルチキャスト経路	-	8,192 (8k)	-	-
	ARP	32,768 (32k)	32,768 (32k)	-	8,192 (8k)
IPv6	ユニキャスト経路※1	16,384 (16k)	16,384 (16k)	-	-
	マルチキャスト経路	-	8,192 (8k)	-	-
	NDP	8,192 (8k)	8,192 (8k)	-	-

(凡例) -:エントリなし

注

PSU-2，PSU-22，PSU-33 のテーブルエントリ配分パターンを選択され PSU-1，PSU-12 および PSU-43 を搭載した場合，搭載した PSU-1，PSU-12 および PSU-43 のテーブルエントリの配分パターンは，PSU-1，PSU-12 および PSU-43 の初期時のパターンとなります。初期時のパターンは，「コンフィグレーションコマンドレファレンス Vol.1　3. 装置管理情報」コンフィグレーションコマンド system の psu_resource のパラメータ省略時の初期値を参照してください。

注※ 1

アクティブ経路

注※ 2

装置の管理には RM イーサネットを使用することを想定しています。

表 3-12　PSU-33 専用のテーブルエントリの配分パターン

想定する利用形態		パターン名	
		l3switch-31	l3switch-32
		キャリア L3 スイッチ IPv4 フルルート (FDB 重視)	キャリア L3 スイッチ IPv4 フルルート (IPv6 重視)
L2	FDB	65,536 (64k)	32,768 (32k)
IPv4	ユニキャスト経路※	262,144 (256k)	262,144 (256k)
	マルチキャスト経路	8,192 (8k)	8,192 (8k)
	ARP	65,536 (64k)	65,536 (64k)
IPv6	ユニキャスト経路※	32,768 (32k)	65,536 (64k)
	マルチキャスト経路	8,192 (8k)	8,192 (8k)
	NDP	16,384 (16k)	32,768 (32k)

注

PSU-33 専用のテーブルエントリ配分パターンを選択され PSU-1，PSU-12，PSU-2，PSU-22 および PSU-43 を搭載した場合，搭載した PSU-1，PSU-12，PSU-2，PSU-22，および PSU-43 のテーブルエントリの配分パターンは，PSU-1，PSU-12，PSU-2，PSU-22 および PSU-43 の初期時のパターンとなります。初期時のパターンは，「コンフィグレーションコマンドレファレンス Vol.1　3. 装置管理情報」コンフィグレーションコマンド system の psu_resource のパラメータ省略時の初期値を参照してください。

注※

アクティブ経路

(2) VLAN

VLAN 最大数は，ポート当たり 4,095，装置当たり 4,095※です。Tag-VLAN 連携を含む通信用の NIF のインタフェースおよびトンネルインタフェースの定義数も，装置当たりの数にカウントします。IEEE802.1Q で規定されている VLAN ID（0 ～ 4,095）のうち“0”は，本装置では使用できません。

また，“1”はデフォルト VLAN として装置内で使用します。このため，コンフィグレーションによって設定が可能な VLAN 数は 4,094 個となります。

本装置で同時に使用可能な VLAN 数は各 VLAN に設定するポート数の合計 (Tagged ポートの場合は該当ポートに設定する VLAN 数分をカウントします) に依存します。例えば，4,095 個の VLAN で，各 VLAN に Tagged ポートを 10 ポートずつ設定する場合，4,095 × 10 ＝ 40,950 と換算します。本装置では，100,000 ポート分まで動作可能です。

プロトコル VLAN 最大数は，装置全体で 96 個です。また，プロトコル VLAN に設定できるポート数は装置全体で 96 ポートです (同じポートに複数の VLAN を tagged-port 指定しても，1 ポートでカウントします)。

注※

VLAN 数 (デフォルト VLAN 含む) と Tag-VLAN 連携を含む通信用の NIF インタフェース，Null インタフェース，トンネルインタフェースの数の合計が 4,096 以内になるようにしてください。

（3） プロトコル VLAN のプロトコル識別数

プロトコル VLAN では，以下のフィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって指定できるプロトコルの種類の最大数はポート当たり 16，装置当たり 16 です。

- EthernetV2 形式フレームの Ether-type 値
- 802.3 形式フレームの LLC 値 (DSAP,SSAP)
- 802.3 形式フレームの Ether-type 値

（4） MAC VLAN

MAC VLAN として使用可能な VLAN 数は 4,094 個（VLAN 2 ～ 4,095）です。

装置当たり設定可能な MAC アドレスのエントリ数は次のとおりです。

（a） BCU メモリが 512MByte 以上の場合

- コンフィグレーションによる静的な設定は 5,000 エントリ
- レイヤ 2 認証機能による動的な設定は 8,192 エントリ

合計 13,192 エントリです。

（b） BCU メモリが 256MByte の場合

- コンフィグレーションによる静的な設定は 1,000 エントリ
- レイヤ 2 認証機能は使用できません。

同じ MAC アドレスをコンフィグレーションとレイヤ 2 認証機能で設定した場合は，それぞれ 1 エントリとカウントします。

（5） アップリンク VLAN

VLAN 当たりのアップリンクポートは最大 8 ポートです。

（6） アップリンクブロック

VLAN 当たりのブロックポートは最大 8 ポートです。

（7） プライベート VLAN

Primary VLAN 当たりの Secondary VLAN 数は最大 8 個です。

(8) Tag-VLAN 連携機能

Tag-VLAN 連携機能で使用する Tag-VLAN 数の最大数は，ポート当たり 4,096(Tag なし VLAN を 1 個含む)，装置当たり 4,096 です。

(9) FDB

FDB に登録できる MAC アドレスのエントリの最大数を次の表に示します。FDB の最大エントリ数はコンフィグレーションによって変更できます。「(1) PSU の最大テーブルエントリ数」を参照してください。

なお，1 エントリを装置として運用中に使用することがあるため，実際に FDB として登録できるエントリ数は最大数から 1 減算した値となります。また，リンクアグリゲーションを使用している場合は，更に最大 7 エントリを装置として使用することがあります。

表 3-13 FDB に登録できる MAC アドレスのエントリ数

モデル	PSU-1，PSU-12，PSU-43		PSU-2，PSU-22，PSU-33	
	PSU 当たり 最大エントリ数	装置当たり 最大エントリ数	PSU 当たり 最大エントリ数	装置当たり 最大エントリ数
SB-7804S	131,072 (1,000)	131,072 (1,000)	262,144 (1,000)	262,144 (1,000)
SB-7808S				
SB-7816S				

注 ( ) 内はその中でスタティックエントリとして登録可能な数です。

(10) リンクアグリゲーション

リンクアグリゲーショングループ当たりの最大ポート数は 16 です。

装置当たりのリンクアグリゲーショングループ数は，128 です。

(11) スパニングツリー

PVST+ 数 (VLAN 数と回線数の積) の最大数は，1,000 です。

PVST+ を 100 個の VLAN で動作させ，それぞれの VLAN に 10 回線が所属している場合，PVST+ 数は 100 × 10 = 1,000 となります。

シングルスパニングツリーを使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，10,000 です。シングルスパニングツリーと PVST+ を併用する場合は，上記 PVST+ 数との合計の最大値が 5,000 となります。

マルチプルスパニングツリーを使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，10,000 です。シングルスパニングツリーまたは PVST+ と併用できません。各 MST インスタンス (MST インスタンス 0 は除く) に対応付けできる VLAN 数の最大数は，200 です。

ただし，各 MST インスタンス (MST インスタンス 0 は除く) に対応できる VLAN 数の最大数は，装置に実装している物理ポート数，および VLAN トンネリング機能を使用している場合と使用していない場合で次の表に示すように異なります。表中の全物理回線数とは装置に実装している物理ポート数の総数を指します。なお，CIST に所属する VLAN 数には制限はありません。

表 3-14　各 MST インスタンスに対応できる VLAN 数 (VLAN トンネリング機能未使用時)

全物理回線数	一つの MST インスタンスに設定できる最大 VLAN 数
216 以下	200 以内
240 以下	160 以内
241 以上	120 以内

表 3-15　各 MST インスタンスに対応できる VLAN 数 (VLAN トンネリング機能使用時)

全物理回線数	一つの MST インスタンスに設定できる最大 VLAN 数
12 以下	80 以内
24 以下	30 以内
36 以下	20 以内
48 以下	10 以内
96 以下	5 以内
97 以上	0 (CIST だけで運用してください)

（12）GSRP

GSRP でレイヤ 3 冗長切替機能を使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，10,000 です。

（13）基本制御モジュール (BCU) のメモリ量と収容経路エントリ数

基本制御モジュールのメモリ量に関する基本方針は，最小メモリ量で最小のエントリ数・インタフェース数・PVST+ 数で動作可能とし，メモリを増設すると使用可能なエントリ数・インタフェース数・PVST+ 数が増加するようにしています。基本制御モジュールのメモリ量と，それに応じて収容できる IP ユニキャストの経路エントリ数，IP マルチキャストの経路エントリ数，IP インタフェース数，およびフィルタ /QoS エントリ数を「表 3-17　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，BGP4 は使用しない）」～「表 3-26　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（2/2）」に示します。

基本制御モジュールを二重化している場合は，運用系 BCU と待機系 BCU の両方に最小所要メモリ量になるようメモリ増設が必要です。

経路エントリ数と隣接ルータ数 / 隣接ピア数の関係については，「（17）ルーティングリソース」の収容条件も参照願います。

- 使用する機能により収容可能な経路エントリ数の条件が変わります。
- BGP4/BGP4+ を使用する場合は，別途対応するオプションライセンス OP-BGP が必要です。
- IS-IS を使用する場合は，別途対応するオプションライセンス OP-ISIS が必要です。
- IPv4 マルチキャスト /IPv6 マルチキャストを使用する場合は，別途対応するオプションライセンス OP-MLT が必要です。
- SB-5400S で OSPF/OSPFv3 を使用する場合は，別途対応するオプションライセンス OP-OSPF が必要です。
- 最大経路エントリ数のアクティブ数は，以下の式を満たすように使用してください。
  BGP4/BGP4+ を使用しない場合は，以下の式から BGP4/BGP4+ を外して考えます。

  IPv4 の場合，

アクティブ数 ≧ (RIP，OSPF，BGP4，IS-IS，スタティックを合わせたアクティブ経路数) ＋ IPv4 インタフェース数× 2(直結経路 (ホスト経路とサブネット経路))
かつ
「表 3-10　PSU-1，PSU-12，PSU-2，PSU-22，PSU-33，PSU-43 で共通のテーブルエントリの配分パターン」，「表 3-11　PSU-2，PSU-22，PSU-33 で共通のテーブルエントリの配分パターン」と「表 3-12　PSU-33 専用のテーブルエントリの配分パターン」の配分パターンの IPv4 ユニキャストエントリ経路数に関し
IPv4 ユニキャストエントリ経路数 ≧
アクティブ数 ＋ ARP エントリ数 ＋ IPv4 インタフェース数× 2 ＋ 3

IPv6 の場合，

アクティブ数 ≧ (RIPng，OSPFv3，BGP4+，IS-IS，スタティックを合わせたアクティブ経路数) ＋ IPv6 インタフェース数× 2(直結経路のグローバルアドレス (ホスト経路とサブネット経路))
かつ
「表 3-10　PSU-1，PSU-12，PSU-2，PSU-22，PSU-33，PSU-43 で共通のテーブルエントリの配分パターン」，「表 3-11　PSU-2，PSU-22，PSU-33 で共通のテーブルエントリの配分パターン」と「表 3-12　PSU-33 専用のテーブルエントリの配分パターン」の配分パターンの IPv6 ユニキャストエントリ経路数に関し
IPv6 ユニキャストエントリ経路数 ≧
アクティブ数 ＋ NDP エントリ数 ＋ IPv6 インタフェース数× 3 (直結経路のリンクローカルアドレス (ホスト経路とサブネット経路) とリンクローカルマルチキャストアドレス一つ)

- 特に注がない場合はマルチパス数は 8 です。
- 最大経路エントリ数には，スタティック経路，ダイレクト経路，集約経路，デフォルト経路，およびループバック経路を含みます。
- NetFlow 統計は QoS とエントリを共用します。したがって，NetFlow 統計で使用しているエントリ数と QoS で使用しているエントリ数の合計が，QoS エントリの最大数を超えた設定はできません。

[表の見方]

表の項目に記載の経路エントリ数は，「基本制御モジュールのメモリ量に応じた収容可能な」IP ユニキャストの経路エントリ数，IP マルチキャストの経路エントリ数，IP インタフェース数，およびフィルタ／ QoS エントリ数を示します。
インタフェース数で IPv4/IPv6 インタフェース数と記載のある場合，IPv4 と IPv6 は独立に数え，値が 4,096 であれば，IPv4 のアドレスを設定したインタフェースの最大値が 4,096，IPv6 のアドレスを設定したインタフェースの最大値が 4,096 を意味します。
また，インタフェース数は IPv4 と IPv6 のインタフェース数の合計値の最大値を示します。
なお，「表 3-17　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，BGP4 は使用しない）」～「表 3-26　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（2/2）」の注意事項は，「表 3-26　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（2/2）」の後ろに記述しています。

(a) PSU-1，PSU-12 および PSU-43/PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l3switch-11/l3switch-12，PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l3switch-21/l3switch-22 の場合

l3switch-11，l3switch-21 にはマルチキャストの条件はありませんので，次の表に示すマルチキャストの条件を外した値が BCU の最小所要メモリ収容条件となります。

● BGP4 ／ BGP4+【**OP-BGP**】を使用しない場合

表 3-16 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，BGP4 は使用しない）

BCU 最小所要メモリ量	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数※8	フィルタ /QoS エントリ数※9	PVST+ 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数		ARP エントリ数	PIM-SM/SSM または PIM-DM※3				
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	スタティック		(S,G) エントリ数	インタフェース数※4			
256MB ※10	※7									
	3,768	3,768	3,000	256	8,192	-	-	256	2,000	128
512MB	42,288	42,288	30,000	4,096	32,768	※5		4,096	20,000	1,000
768MB									50,000	
1024MB									100,000 ※1	

（凡例） - : 該当なし

基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ は使用しない）の表の (1/2) と (2/2) を次に示します。

表 3-17 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ は使用しない）（1/2）

BCU 最小所要メモリ量	IPv4 ユニキャスト					IPv4 マルチキャスト	
	最大経路エントリ数		プロトコル別最大経路エントリ数		ARP エントリ数	PIM-SM/SSM または PIM-DM※3	
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	スタティック		(S,G) エントリ数	インタフェース数※4
256MB ※10	※7						
512MB	22,288	22,288	10,000	4,096	32,768	1,000	64
						3,000	32
	42,288	42,288	30,000	4,096	32,768	※5	
768MB						※5	
1024MB						※5	

表 3-18 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ は使用しない）(2/2)

BCU 最小所要メモリ量	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv4/IPv6 インタフェース数※8	フィルタ/QoS エントリ数※9	PVST+ 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数		NDP エントリ数	PIM-SM/SSM				
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPF v3 +IS-IS	スタティック		(S,G) エントリ数	インタフェース数※4			
256MB ※10	※7									
512MB	16,144	16,144	10,000	2,048	8,192	500	2,048	4,096	20,000	1,000
	16,144	16,144	10,000	2,048	8,192	※5		4,096	20,000	1,000
768MB									50,000	
1024MB									100,000 ※1	

● BGP4 ／ BGP4+**【OP-BGP】**を使用する場合

表 3-19 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，BGP4 を使用する）

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト		IPv4 インタフェース数※8	フィルタ / QoS エントリ数※9	PVST+ 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数			ARP エントリ数	PIM-SM/SSM				
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※4			
256MB ※10	※7										
512MB	45,000	45,000	30,000	45,000	4,096	32,768	※5		4,096	20,000	1,000
768MB										50,000	
1024MB										100,000 ※1	

基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）の表の (1/2) と (2/2) を次に示します。

表 3-20　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（1/2）

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト	
	最大経路エントリ数		プロトコル別最大経路エントリ数			ARP エントリ数	PIM-SM/SSM	
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※4
256MB ※10	※7							
512MB	25,000	25,000	10,000	25,000	4,096	32,768	-	-
	45,000	45,000	30,000	45,000	4,096	32,768	※6	
768MB							※6	
1024MB							※6	

（凡例） - : 該当なし

表 3-21　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（2/2）

BCU 最小所要メモリ量	IPv6 ユニキャスト						IPv6 マルチキャスト		IPv4/IPv6 インタフェース数※8	フィルタ /QoS エントリ数※9	PVST+ 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数			NDP エントリ数	PIM-SM/SSM				
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPF v3 +IS-IS	BGP4 +	スタティック		(S,G) エントリ数	インタフェース数※4			
256MB ※10	※7										
512MB	16,384	16,384	10,000	16,384	2,048	8,192	500	2,048	4,096 ※2	20,000	1,000
	16,384	16,384	10,000	16,384	2,048	8,192	※6				
768MB							※6			50,000	
1024MB							※6			100,000 ※1	

(b) PSU-1，PSU-12 および PSU-43/PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l2switch-12，PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l2switch-22 の場合

表 3-22 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，BGP4 は使用しない）

BCU 最小所要メモリ量	IPv4 ユニキャスト					IPv4 インタフェース数※8	フィルタ/QoS エントリ数※9	PVST+ 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数		ARP エントリ数			
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	スタティック				
256MB ※10	3,768	3,768	3,000	256	8,192	256	2,000	128
512MB							20,000	1,000
768MB							50,000	
1024MB							100,000 ※1	

(c) PSU-1，PSU-12 および PSU-43/PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l2switch-11，PSU-2 および PSU-22/PSU-33 のテーブルエントリ数の配分パターン l2switch-21 の場合

本条件の場合は，フィルタ／ QoS エントリ数だけの条件となります。

表 3-23 基本制御モジュールのメモリ量とフィルタ／ QoS エントリ数

BCU 最小所要メモリ量	フィルタ／ QoS エントリ数※9	PVST+ 総回線数
256MB ※10	2,000	128
512MB	20,000	1,000
768MB	50,000	
1024MB	100,000 ※1	

(d) PSU-33 のテーブルエントリ数の配分パターン l3switch-31/l3switch-32 の場合

基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）の表の (1/2) と (2/2) を次に示します。

表 3-24 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（1/2）

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト	
	最大経路エントリ数		プロトコル別最大経路エントリ数			ARP エントリ数	PIM-SM/SSM	
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※4
1024MB	520,000	262,144	30,000	520,000	4,096	65,536	※6	

表 3-25 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，BGP4/BGP4+ を使用する）（2/2）

BCU 最小所要メモリ量	IPv6 ユニキャスト						IPv6 マルチキャスト		IPv4/IPv6 インタフェース数	フィルタ /QoS エントリ数※9	PVST + 総回線数
	最大経路エントリ数		プロトコル別最大経路エントリ数			NDP エントリ数	PIM-SM/SSM				
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPF v3 +IS-IS	BGP4+	スタティック		(S,G) エントリ数	インタフェース数※4			
1024 MB	100,000	65,536	10,000	100,000	4,096	32,768	※6		4,096 ※2	100,000 ※1	1,000

注※ 1
装置モデルごとに異なります。詳細は，「(19) フィルタリング・QoS (a) フィルタ /QoS エントリ数」を参照してください。

注※ 2
IPv6 の最大インタフェース数は，2,048 です。

注※ 3
PIM-SM/SSM と PIM-DM は，同時に動作できません。(注※ 5) に示す (S，G) エントリ数とインタフェース数の組み合わせで使用するメモリ量は PIM-SM/SSM と PIM-DM は同じです。

注※ 4
PIM-SM/SSM の場合，使用可能なインタフェース数は，表中の (数値 -1) です。32 であれば 31 までです。また，このインタフェース数はコンフィグレーションコマンド (pim コマンド max-interfaces サブコマンド，pim6 コマンド max-interfaces サブコマンド) により指定してください。指定しない場合，デフォルト値は 256 です。

注※ 5
(S，G) エントリ数とインタフェース数の組み合わせは，以下のどれかの組み合わせでご使用ください。ただし，2,048 インタフェースは IPv6 PIM-SM 使用時だけ可能です。

表 3-26 （S,G）エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
8,000	32
5,000	64
3,000	128

(S,G) エントリ数	インタフェース数
1,000	256
250	2,048

注※ 6

IPv4 と IPv6 のマルチキャストに関し，(S，G) エントリ数とインタフェース数は IPv4 と IPv6 の合計値が（注※ 5）のエントリ数以内となるようにご使用ください。

注※ 7

IPv4 ユニキャスト，IPv4 マルチキャスト，IPv6 ユニキャスト，IPv6 マルチキャスト，ARP，NDP，フィルタ / QoS，インタフェース数，PVST+ 数は最小値であれば，同時に動作可能です。

注※ 8

VLAN 定義に関しては IP 定義の有無に関わらず，IP インタフェースを消費します。

注※ 9

NetFlow 統計は QoS とエントリを共用します。したがって，NetFlow 統計で使用しているエントリ数と QoS で使用しているエントリ数の合計が，QoS エントリの最大数を超えた設定はできません。

注※ 10

256MB を搭載する場合は下記をご注意ください。

記載されている各機能のすべてのエントリ数の収容で，オンラインによる下記のコンフィグレーションの追加／削除／変更を実施する場合は搭載メモリを 512MB 以上で運用してください。

1. 装置管理情報
2. SNMP 情報
3. 回線（Line）情報
4. リンクレイヤプロトコル情報
5. トンネル情報
6. レイヤ 2 スイッチ情報
7. IP インタフェース情報
8. IP ルーティングプロトコル情報
9. IP マルチキャストルーティングプロトコル情報
10. フロー情報
11. QoS 情報
12. デフォルト情報
13. VRRP 情報
14. RA 情報
15. ホスト名情報
16. ログ情報
17. NTP 情報
18. Disable 情報

（14）インタフェース数

IPv4 アドレス，および IPv6 アドレスを付与する単位をインタフェースと呼びます。そのインタフェース数の最大値は，装置当たり 4,096 です。IPv4 と IPv6 インタフェース数は独立して数え，IPv4 と IPv6 のインタフェース数の合計値が最大インタフェース数を超えないように使用してください。本値に含むインタフェースは，Tag-VLAN 連携を含む通信用の NIF のインタフェース，VLAN インタフェース，Null インタフェース，トンネルインタフェースを含みます。RM イーサネット通信インタフェース，AUX 通信インタフェースの数は含みません。また，最大インタフェース数での動作はスタティックルートを前提にしています。RIP，OSPF などのダイナミックルーティングの場合は，ルーティングプロトコルが動作する

インタフェース数が最大隣接ルータ数の制限内になるように使用してください。詳細は「表 3-30　最大隣接ルータ数」を参照してください。

(a) 最大トンネルインタフェース数

IPv6 over IPv4 トンネルインタフェース数は，装置当たり最大 256 です。IPv4 over IPv6 トンネルインタフェース数は，装置当たり最大 256 です。6to4 トンネルインタフェース数は，装置当たり最大 1 です。また，IPv6 over IPv4 トンネル，IPv4 over IPv6 トンネル，および 6to4 トンネルのインタフェース数の合計値は，装置当たり最大 256 です。

(15) アドレス数

コンフィグレーションで設定できる IPv4 アドレスの最大数は，4,096 です。本値は，マルチホーム，Tag-VLAN 連携を含む通信用の NIF のインタフェース，VLAN インタフェースおよびトンネルインタフェースに設定できる IPv4 アドレス数です。RM イーサネット通信インタフェース，および AUX 通信インタフェースに設定できる IPv4 アドレス数は含みません。

また，コンフィグレーションで設定できる IPv6 アドレスの最大数は，2,048 です。この値は，マルチホーム，Tag-VLAN 連携を含む通信用の NIF のインタフェースおよびトンネルインタフェースに設定できる IPv6 アドレス数です。

(a) マルチホームの最大アドレス数

LAN のマルチホーム接続では一つのインタフェースに対して，複数の IPv4 アドレス，または IPv6 アドレスを設定できます。

マルチホーム接続においてコンフィグレーションで設定できる IPv4 最大アドレス数は，インタフェース当たり最大 256，IPv6 最大アドレス数は，インタフェース当たり最大 7 です。

なお，IPv6 の場合，一つのインタフェースには必ず一つのリンクローカルアドレスが設定されるため，マルチホーム接続でインタフェースに IPv6 グローバルアドレスだけ定義した場合，実際に装置に設定される IPv6 アドレス数は，自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 となります。

(16) 最大相手装置数

本装置が直接収容する LAN を介して IP 通信できる最大相手装置数を示します。この場合の相手装置はルータに限らず端末も含みます。

(a) ARP エントリ数，NDP エントリ数

イーサネットでは，ARP，NDP などのアドレス解決によって，送信しようとするパケットの宛先 IP アドレスに対応するハードウェアアドレスを決定します。したがって，ARP エントリ数，NDP エントリ数によって最大相手装置数が決まります。ARP エントリ数，NDP エントリ数を次の表に示します。

表 3-27　ARP エントリ数，NDP エントリ数

項目	最大エントリ数（装置当たり）
ARP	32,768
NDP	8,192

注 1

ダイナミックエントリとスタティックエントリの最大エントリ数については，「表 3-57　ダイナミック・スタティック最大エントリ数」を参照してください。

注 2

全エントリを 1 インタフェースで使用することもできます。

注 3

ARP と NDP は独立動作です。それぞれ最大エントリ数を使用できます。

(b) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 3-28　RA の相手端末数

項目	最大相手端末数
RA	4,096

注

相手端末数に応じて RA の送信間隔は制限されます。詳細は,「コンフィグレーションコマンドレファレンス Vol.1　11. RA 情報」のコンフィグレーションコマンド ra を参照してください。

(17) ルーティングリソース

(a) 最大隣接ルータ数

最大隣接ルータ数を「表 3-30　最大隣接ルータ数」に示します。最大隣接ルータ数の定義はルーティングプロトコルによって異なります。各プロトコルの最大隣接ルータ数の定義を「表 3-32　最大隣接ルータ数の定義」に示します。

表 3-29　最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数
スタティックルーティング (IPv4，IPv6 の合計)	4,096 ※
OSPF	200
OSPFv3	100
IS-IS	50
RIP，OSPF，BGP4，RIPng，OSPFv3，BGP4+，IS-IS の合計	256

注※

動的監視機能を使用する隣接ルータは，ポーリング間隔によって数が制限されます。詳細は，次の表のスタティックの動的監視機能を使用できる最大隣接ルータ数を参照してください。

表 3-30　スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
5 秒	300
10 秒	600
20 秒	1,200

表 3-31　最大隣接ルータ数の定義

ルーティングプロトコル	定義
スタティックルーティング	ネクストホップ・アドレスの数

ルーティングプロトコル	定義
RIP	RIP が動作するインタフェース数※
RIPng	RIPng が動作するインタフェース数※
OSPF	OSPF が動作する各インタフェースにおける下記の総計 1. 該当するインタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当するインタフェースと接続されるほかの OSPF ルータの数 2. 該当するインタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当するインタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンドの show ip ospf neighbor コマンドで表示される隣接ルータの状態（State）が「Full」となる隣接ルータの数と同じ意味になります。
OSPFv3	OSPFv3 が動作する各インタフェースにおける下記の総計 1. 該当するインタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当するインタフェースと接続されるほかの OSPFv3 ルータの数 2. 該当するインタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当するインタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンドの show ipv6 ospf neighbor コマンドで表示される隣接ルータの状態（State）が「Full」となる隣接ルータの数と同じ意味になります。
BGP4	BGP4 ピア数
BGP4+	BGP4+ ピア数
IS-IS	本装置と接続されるほかの IS-IS ルータの数

注※

コンフィグレーションのインタフェースパラメータを省略した場合はすべてのインタフェースが対象になります。

(b) 経路エントリ数と最大隣接ルータ数の関係

経路エントリ数と最大隣接ルータ数（RIP/RIPng，OSPF/OSPFv3，IS-IS），経路エントリ数と最大ピア数 (BGP,BGP4+) の関係を「表 3-33　経路エントリ数と最大隣接ルータ数の関係」～「表 3-35　経路エントリ数と最大ピア数の関係 (IPv4，IPv6 混在)【OP-BGP】」に示します。

なお，最大隣接ルータ数は本装置より経路広告を行うルータ数となります。

表 3-32　経路エントリ数と最大隣接ルータ数の関係

ルーティング プロトコル	最大経路 エントリ数※1	最大隣接ルータ数	備考
RIP	1,000	100	※2
RIPng	1,000	100	
OSPF※3	1,000	200	
	2,000	100	
	5,000	40	
	10,000	20	
	20,000	10	
	30,000	6	
OSPFv3※3	1,000	100	
	2,000	50	
	5,000	20	
	10,000	10	
IS-IS※4	1,000	50	
	2,000	25	
	5,000	10	
	10,000	5	

注※ 1
最大経路エントリ数は代替経路を含みます。

注※ 2
各ルーティングプロトコル (RIP，RIPng，OSPF，OSPFv3，IS-IS，BGP4，BGP4+) を併用して使用する場合の最大隣接ルータ数は，各々 1/n(n：使用ルーティングプロトコル数) となります。例えば，BGP，BGP4+ を使用せず，OSPF(5,000 経路) と OSPFv3(5,000 経路) を併用して使用する場合の最大隣接ルータ数は，1/2 である，OSPF では 20，OSPFv3 では 10 となります。

注※ 3
OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※ 4
IS-IS の最大経路エントリ数は，IPv4 経路エントリ数と IPv6 経路エントリ数の合計とします。

表 3-33　経路エントリ数と最大ピア数の関係（IPv4 だけ）【OP-BGP】

ルーティングプロトコル	上位ピア数※1	BCU の実装メモリ	最大経路エントリ	最大隣接ピア数 ※2※3※4※5
BGP4	2	512MB	22,500	256
		768MB	22,500	256
		1024MB	22,500	256
		1024MB※6	200,000	256
	3	512MB	15,000	256
		768MB	15,000	256
		1024MB	15,000	256
		1024MB※6	160,000	256

ルーティングプロトコル	上位ピア数※1	BCU の実装メモリ	最大経路エントリ	最大隣接ピア数 ※2※3※4※5
	4	512MB	11,250	256
		768MB	11,250	256
		1024MB	11,250	256
		1024MB※6	120,000	256

表 3-34　経路エントリ数と最大ピア数の関係 (IPv4，IPv6 混在)【OP-BGP】

ルーティングプロトコル	上位ピア数※1	BCU の実装メモリ	最大経路エントリ		最大隣接ピア数 ※2※3※4※5
			IPv4	IPv6	
BGP4 BGP4+	2	512MB	22,500	8,192	128
		768MB	22,500	8,192	128
		1024MB	22,500	8,192	128
		1024MB※6	200,000	40,000	128
	3	512MB	15,000	5,461	64
		768MB	15,000	5,461	128
		1024MB	15,000	5,461	128
		1024MB※6	160,000	32,000	128
	4	512MB	11,250	4,096	32
		768MB	11,250	4,096	128
		1024MB	11,250	4,096	128
		1024MB※6	120,000	24,000	128

注※1
　上位ピア数とは，最大経路エントリ数を広告してくるピアの数を示します。

注※2
　最大隣接ピア数とは，上位ピアから受信した経路を広告するピアの数を示します。表に示す値はマルチキャスト未使用で，かつマルチパス数が4，送受信フィルタリングによる属性変更なしの場合の値です。

注※3
　BGP4 と BGP4+ は独立動作です。BGP4 と BGP4+ それぞれでこの表に示す最大隣接ピア数を使用できます。

注※4
　「最大隣接ピア数 =0」は「上位ピアからの BGP 経路を受け取ることはできるが，隣接ピアに広告することはできない」ことを意味します。

注※5
　「最大隣接ピア数 = ×」は「上位ピアからの BGP 経路を受け取ることができない」ことを意味します。

注※6
　PSU-33 を使用の場合です。

(18) IPv4/IPv6 マルチキャスト【OP-MLT】

IPv4/IPv6 マルチキャスト定義できるインタフェース数およびマルチキャスト経路情報のエントリ数を次の表に示します。マルチキャスト経路情報のエントリ数とインタフェース数によって必要となる搭載メモリ量が異なります。

本装置は IPv4 マルチキャストルーティングプロトコルとして PIM-SM，PIM-SSM，PIM-DM および DVMRP をサポートします。ただし，PIM-SM と PIM-SSM 以外のプロトコルは同時には動作しません。IPv6 マルチキャストルーティングプロトコルとして PIM-SM，および PIM-SSM をサポートします。

IPv4 マルチキャストと IPv6 マルチキャストは同時に動作でき，かつ PIM-SM と PIM-SSM は同時に動作できます。

表 3-35　IPv4/IPv6 マルチキャストの最大数

項目	IPv4 最大数	IPv6 最大数
PIM-SM/SSM マルチキャストインタフェース数	255 ／装置※1 ※2	255 ／装置※3 ※4
IGMP/MLD 動作インタフェース数	4,095 ／装置※5 ※6 ※7	2,047 ／装置※3 ※6 ※7
1 グループ当たりの送信元数	256 ／グループ	256 ／グループ
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ，(*,G) エントリ，およびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	8,000 ／装置	8,000 ／装置※8
PIM-DM/DVMRP マルチキャスト経路情報のエントリ ((S,G) エントリおよびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	8,000 ／装置	-
IGMPv2/IGMPv3(EXCLUDE モード) / MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連携動作させる設定数	1,024 ／装置※9	256 ／装置※10
IGMPv3/MLDv2 における Report 内に格納できるグループ情報	32 record ／メッセージ 32 ソース／ record	32 record ／メッセージ※11 32 ソース／ record
IGMP/ MLD 加入グループ数※12	IGMP 256 ／装置※13	MLD 256 ／装置※13
マルチキャストルータ隣接数	256 ／装置	256 ／装置
ランデブーポイント数	1 ／グループ	1 ／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128 ／装置	128 ／装置
1 システム当たりランデブーポイントで設定できる延べグループ数	128 ／システム	128 ／システム
BSR 候補数	1 ／システム	1 ／システム
1 インタフェース当たりの静的グループ加入数	256 ／インタフェース	1,024 ／インタフェース
静的グループ加入数※14	8,192 ／装置※15	8,192 ／装置
静的ランデブーポイントルータアドレス数	16 ／装置	16 ／装置
IGMP/ MLD グループ当たりのソース数	256 ／グループ	256 ／グループ
(S,G) エントリ当たりの出力物理ポート延べ数※16	max-interfaces が 256 以下の場合 384 ／エントリ max-interfaces が 4,096 の場合 4,096 ／エントリ	max-interfaces が 256 以下の場合 384 ／エントリ max-interfaces が 4,096 の場合 4,096 ／エントリ
PIM-DM マルチキャストインタフェース数	256 ／装置※1	-
DVMRP マルチキャストインタフェース数	32 ／装置※1 ※17	-

（凡例） -：該当なし

注※ 1

マルチホームはサポートしていません。

注※ 2

PIM-SM インタフェースと PIM-SSM インタフェースの合計で 255/ 装置です。

注※ 3

マルチホームもサポートしています。

注※ 4

IPv6 マルチキャストインタフェースとして，このほかにカプセル化用インタフェースが一つ存在します。このため，IPv6 PIM-SM マルチキャストインタフェース全体の数は 256 個になりますが，ユーザが設定できるのはそのうち 255 個です。また，PIM-SM と PIM-SSM の合計で 255 個となります。

注※ 5

使用するマルチキャストルーティングプロトコルによって異なります。

- PIM-SM/PIM-SSM：4,095
- PIM-DM：256
- DVMRP：32

注※ 6

256 インタフェース以上を使用する場合は，動作できる PIM-SM/PIM-SSM マルチキャストインタフェース数は 31 までとなります。

注※ 7

256 インタフェース以上で使用する場合，BCU の搭載メモリ量は 1024MB 必要となります。

注※ 8

256 インタフェース以上を使用する場合は，登録できるエントリ数は 500 までとなります。

注※ 9

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-37　使用インタフェース数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-38　加入グループ数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。

表 3-36　使用インタフェース数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定数
31	1,024
63	512
127	512
255	256
4,095	64

表 3-37　加入グループ数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数（のべ数）	IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定数
16	1,024
32	512
64	256
128	128
256	64
512	32
1,024	16
2,048	8
4,096	3
8,192	1

加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つでなく，加入したインタフェースの数になります。一つの IGMPv3（EXCLUDE モード）Report で PIM-SSM を連携動作させる設定数は 256 になります。例えば，一つの IGMPv3（EXCLUDE モード）Report 内に三つの record がある場合，それぞれの record に対応する PIM-SSM を連携動作させる設定数の合計が 256 を超えたときは，以降の record に対する本設定は無視します。

注※ 10

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-39　使用インタフェース数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-40　加入グループ数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。

表 3-38　使用インタフェース数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256
255	256
2,047	64

表 3-39　加入グループ数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数（のべ数）	MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128

加入グループ数（のべ数）	MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定数
256	64
512	32
1,024	16
2,048	8
4,096	4
8,192	2

加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つでなく，加入したインタフェースの数になります。一つの MLDv2（EXCLUDE モード）Report で PIM-SSM を連携動作させる設定数は 256 になります。例えば，一つの MLDv2（EXCLUDE モード）Report 内に三つの record があり，各 record に対応する PIM-SSM を連携動作させる設定数の合計が 256 を超えた場合，以降の record に対する本設定は無視します。

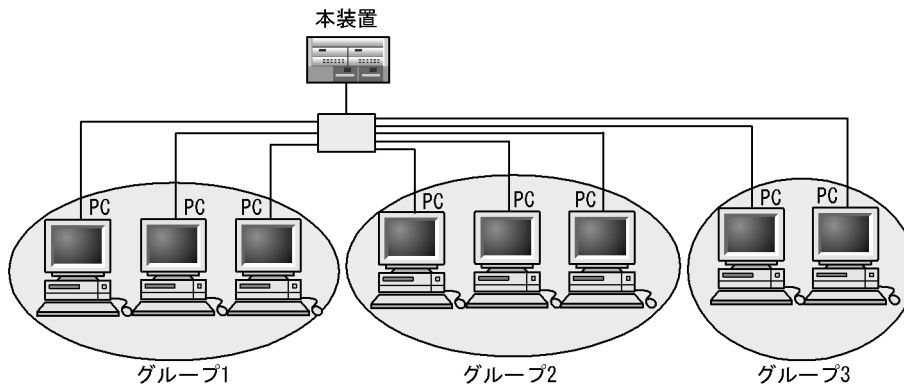
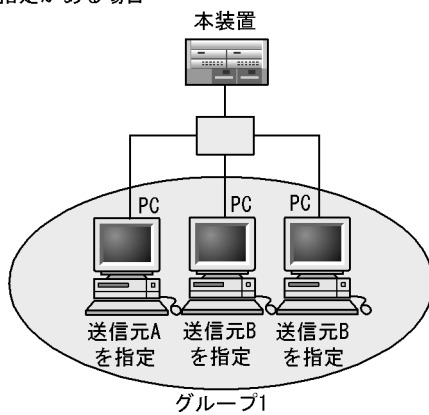
注※ 11

一つの Report メッセージで処理できるソース数は延べ 1,024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。
MLDv2 での EXCLUDE モードで SSM に接続する設定をした場合，受信した Report メッセージ内の record のソース数がのべ 1,024 を超えた以降の record は無視します。
例えば，MLDv2EXCLUDE モードで SSM に接続する設定をマスク指定で 1 グループに対し 256 ソースの定義をした場合，次のようになります。

1. 受信した MLDv2 Report メッセージ内の先頭からこの設定に一致する二つの EXCLUDE の record が存在した場合，5record 目以降を無視します。
2. 受信した MLDv2 Report メッセージ内に 1 ソースの INCLUDE の record があり，この設定に一致するグループの EXCLUDE が 4record あった場合，4record 目以降から無視します。

注※ 12

本装置に直接接続しているグループの数です。IGMPv3/MLDv2 使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。
次に示す図の (1) の例では 3 です。(2) の例では (送信元 A，グループ 1) および (送信元 B，グループ 1) の組み合わせになるため，グループ数は 2 になります。

図 3-1　マルチキャストグループ数の例

注※ 13

IPv4 におけるインタフェース当たりの加入可能グループ数を次の表に示します。

表 3-40　IPv4 におけるインタフェース当たりの加入グループ数

マルチキャスト 動作インタフェース数	インタフェース当たりの加入可能グループ数 （グループ＋ソース数）
31	256
63	128
127	64
255	32
4,095	2

IPv6 におけるインタフェース当たりの加入可能グループ数を次の表に示します。

表 3-41　IPv6 におけるインタフェース当たりの加入可能グループ数

マルチキャスト 動作インタフェース数	インタフェース当たりの加入可能グループ数 （グループ＋ソース数）
31 （MLD 動作インタフェース数は 8 まで）	1024 （動的加入グループ数は 256 まで）
31	256
63	128

マルチキャスト 動作インタフェース数	インタフェース当たりの加入可能グループ数 （グループ＋ソース数）
127	64
255	32
2,047	2

注※ 14

静的グループ加入数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総計です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的グループ加入数は一つではなく，静的加入設定したインタフェースの数となります。

注※ 15

PIM-DM または DVMRP は 128/ 装置です。

注※ 16

(S,G) エントリの出力インタフェースが VLAN の場合，1 出力インタフェースに対して物理ポートが複数になる場合があります。この場合の出力物理ポート延べ数は，各出力インタフェースに対する物理ポートの総数となります。
例えば，出力インタフェース数が 2 で，インタフェース当たりの物理ポート数が 5 の場合，出力物理ポート延べ数は 10 となります。

注※ 17

DVMRP を使用する場合は，本装置の全インタフェース数を 500 以下の環境で使用してください。

(a) PIM-SM ／ PIM-SSM ／ PIM-DM 使用時の注意

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

マルチキャストデータの送信元となるサーバの中には，マルチキャストパケットをバーストトラフィックとして送信する特性を持つものがあります。この特性を持つサーバから受信したマルチキャストデータを，マルチキャスト配信する場合には注意が必要です。マルチキャスト配信先の回線を収容するネットワークインタフェースモジュール（NIF）の種類によって，マルチキャスト動作可能なインタフェース数が異なります。マルチキャスト動作可能なインタフェース数を次の表に示します。

表 3-42 マルチキャスト動作可能なインタフェース数（ポート当たり，NIF 当たり）

NIF 略称	マルチキャスト動作可能なインタフェース数（推奨値※ 1）
NE1GSHP-4S	NIF 当たり 1024 インタフェース
NE1GSHP-8S	NIF 当たり 2048 インタフェース※ 2
NE10G-1ER	ポート当たり 8 インタフェース
NE10G-1LW	ポート当たり 8 インタフェース
NE10G-1EW	ポート当たり 8 インタフェース
NE10G-1RX	ポート当たり 8 インタフェース
S12-1G48S	ポート当たり 8 インタフェース
S12-1G48T	ポート当たり 8 インタフェース
S22-10G4RX	ポート当たり 8 インタフェース
S33-10G4RX	ポート当たり 8 インタフェース

NIF 略称	マルチキャスト動作可能なインタフェース数（推奨値※1）
NE1G-12TA	ポート当たり 8 インタフェース
NE1G-48T	8 ポート当たり 8 インタフェース
NE1G-12SA	ポート当たり 8 インタフェース
NE1G-6GA	ポート当たり 8 インタフェース
NEMX-12	ポート当たり 8 インタフェース
NP192-1S	ポート当たり 8 インタフェース
NP192-1S4	ポート当たり 8 インタフェース
NP48-4S	ポート当たり 8 インタフェース

注※ 1

推奨値は，送信元サーバが，マルチキャストパケットを 8 バーストで送信する特性（サーバで 8 パケット分のマルチキャストデータをいったん蓄積した後に，ネットワークに対して連続的に送信する特性）を持っていることを想定しています。バースト数が大きくなると，パケットを一部廃棄することがあるので，マルチキャスト定義するインタフェース数を少なくする必要があります。

注※ 2

キュー長指定機能で，マルチキャストパケットを送信する NIF 側送信キューのキュー長を拡張する必要があります。拡張しない場合，NIF 当たり 1024 インタフェースとなります。キュー長指定機能については，「解説書 Vol.2 1.8.2(4) キュー長指定機能」を参照してください。

(19) フィルタリング・QoS

ここでのエントリ数とは，コンフィグレーションで設定した内容を装置内部で使用する形式 (エントリ) に変換した後の数です。

(a) フィルタ /QoS エントリ数

フィルタおよび QoS のエントリ数は，モデル，BCU 搭載メモリ量，および使用する PSU の種別によって，エントリ数が異なります。

フィルタおよび QoS のエントリ数を次に示します。

表 3-43 SB-7804S の収容条件

BCU 搭載 メモリ量	装置当たり		PSU 当たり					
			フィルタの 最大エントリ数		QoS の 最大エントリ数		フィルタ・QoS 同時使用時の 最大エントリ数	
	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
512MB	20,000	20,000	8,000	16,000	8,000	16,000	16,000	20,000
768MB	32,000	50,000	8,000	16,000	8,000	16,000	16,000	32,000
1024MB	32,000	64,000	8,000	16,000	8,000	16,000	16,000	32,000

表 3-44 SB-7808S の収容条件

BCU 搭載 メモリ量	装置当たり		PSU 当たり					
			フィルタの 最大エントリ数		QoS の 最大エントリ数		フィルタ・QoS 同時使用時の 最大エントリ数	
	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
512MB	20,000	20,000	8,000	16,000	8,000	16,000	16,000	20,000
768MB	50,000	50,000	8,000	16,000	8,000	16,000	16,000	32,000
1024MB	64,000	100,000	8,000	16,000	8,000	16,000	16,000	32,000

表 3-45 SB-7816S の収容条件

BCU 搭載 メモリ量	装置当たり		PSU 当たり					
			フィルタの 最大エントリ数		QoS の 最大エントリ数		フィルタ・QoS 同時使用時の 最大エントリ数	
	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
512MB	20,000	20,000	8,000	16,000	8,000	16,000	16,000	20,000
768MB	50,000	50,000	8,000	16,000	8,000	16,000	16,000	32,000
1024MB	100,000	100,000	8,000	16,000	8,000	16,000	16,000	32,000

フローフィルタ情報およびフロー QoS 情報はフローコンフィグレーションで定義しますが，リストに設定するフロー検出条件パラメータによって使用するエントリ数が異なります。

複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-46 複数エントリを使用するフロー検出条件

複数エントリを使用する フロー検出条件のパラメータの指定	使用エントリ数算出例
宛先 IPv4 アドレス， 送信元 IPv4 アドレス， 宛先 IPv6 アドレス， 送信元 IPv6 アドレス を範囲指定	指定された IP アドレスが幾つのサブネットに区切られるかによって使用エントリ数が決定します。 例えば，宛先 IPv4 アドレスに 192.168.0.1-192.168.0.4 と指定した場合， 192.168.0.1/32, 192.168.0.2/31, 192.168.0.4/32 の三つのサブネットに区切られますので，使用エントリ数は 3 となります。 そのほかも同様です。
宛先 IPv6 アドレス， 送信元 IPv6 アドレスに pd_prefix を指定	IPv6 DHCP サーバ機能によって，指定したインタフェース名で配布可能な IPv6 プレフィックス数が使用エントリ数となります。 例えば，pd_prefix を指定したインタフェース名に，コンフィグレーション dhcp6_server で，100 個のプレフィックスが割り当てられていた場合，使用エントリ数は 100 となります。

複数エントリを使用する フロー検出条件のパラメータの指定	使用エントリ数算出例
宛先ポート番号を範囲指定， 送信元ポート番号を範囲指定， IP ユーザデータ長上限値， IP ユーザデータ長下限値	指定された値が最大 16 ビットのマスクで区切ったときに幾つに分けられるかによって使用エントリ数が決定します。 例えば，宛先ポート番号に 135-140 と指定した場合， 135/16 = 0000 0000 1000 0111(2 進表記） 136/14 = 0000 0000 1000 10xx(2 進表記） 140/16 = 0000 0000 1000 1100(2 進表記） の三つの領域に区切られますので，使用エントリ数は 3 となります。 そのほかも同様です。 なお，IP ユーザデータ長上限値指定時は，0 ～（指定上限値 +20 バイト※1）※2 の範囲指定となります。また，IP ユーザデータ長下限値指定時は，（指定下限値 +20 バイト※1）～ 65,535 までの範囲指定となります。
VLAN 番号を複数指定	設定した VLAN 番号数分エントリを使用します。例えば，vlan 1-2 と指定すると，使用エントリ数は 2 となります。 また，vlan と指定した場合の使用エントリ数は，インタフェース名を指定したときは 1 エントリ，物理ポートを指定したときは，指定した物理ポートが所属する VLAN 数となります。

注※ 1

IP ヘッダ長 20 バイト分を指定値に足して計算を行います。

注※ 2

「指定上限値 + IP ヘッダ長 20 バイト」が 65,535 より大きい場合は，0 ～ 65,535 の範囲指定となります。

● フィルタ機能での 1 リストで使用するエントリ数

1 リストで使用するエントリ数は次のとおりです。

- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを一つ指定した場合，指定したパラメータで使用するエントリ数が，1 リストで使用するエントリ数（「表 3-48　1 リストで使用するエントリ数（フィルタ）」の N）となります。
- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを二つ以上指定した場合，各パラメータで使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数（「表 3-48　1 リストで使用するエントリ数（フィルタ）」の N）となります。
  例えば，1 リストに宛先 IPv4 アドレスの範囲指定と送信元 IPv4 アドレスの範囲指定を指定した場合，「1 リストで使用するエントリ数（「表 3-48　1 リストで使用するエントリ数（フィルタ）」の N）= 宛先 IPv4 アドレスの範囲指定での使用エントリ数×送信元 IPv4 アドレスの範囲指定での使用エントリ数」となります。
- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない場合，使用エントリ数は 1 エントリとなります。

なお，複数 PSU にわたる VLAN，またはリンクアグリゲーションのインタフェースに対して，リストを設定した場合，「1 リストで使用するエントリ数×指定インタフェースがわたる PSU 枚数」分のエントリ数を，装置当たりのエントリ数から消費します。例えば，PSU 1,2,3 にわたる VLAN のインタフェースに 1 リストで使用するエントリ数が 10 エントリとなるリストを指定した場合，10 × 3 ＝ 30 エントリを，装置当たりのエントリ数から消費します。

表 3-47　1 リストで使用するエントリ数（フィルタ）

設定条件	使用エントリ数
「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない	1
「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定	N※

注※　各パラメータで使用するエントリ数を掛け合わせた値

● QoS 機能での 1 リストで使用するエントリ数

1 リストで使用するエントリ数は，重要パケット保護機能を指定した場合，「通常フロー検出条件で使用するエントリ数＋重要フロー検出条件で使用するエントリ数」となります。重要パケット保護機能を使用しない場合は，通常フロー検出条件で使用するエントリ数が，1 リストで使用するエントリ数となります。

通常・重要フロー検出条件で使用するエントリ数は，次のとおりです。

- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを一つ指定した場合，指定したパラメータで使用するエントリ数が 1 リストで使用するエントリ数（「表 3-49　1 リストで使用するエントリ数（QoS)」）となります。
- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを二つ以上指定した場合，各パラメータで使用するエントリ数（「表 3-49　1 リストで使用するエントリ数（QoS)」）を掛け合わせた値となります。
- 「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない場合，使用エントリ数は 1 エントリとなります。

なお，複数 PSU にわたる VLAN，リンクアグリゲーションのインタフェースに対して，リストを設定した場合，「1 リストで使用するエントリ数×指定インタフェースがわたる PSU 枚数」分のエントリ数を，装置当たりのエントリ数から消費します。例えば，PSU 1,2,3 にわたる VLAN のインタフェースに 1 リストで使用するエントリ数が 10 エントリとなるリストを指定した場合，10 × 3 ＝ 30 エントリを，装置当たりのエントリ数から消費します。

表 3-48　1 リストで使用するエントリ数（QoS）

通常フロー検出条件	重要フロー検出条件	使用エントリ数	
		通常フロー検出条件	重要フロー検出条件
「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない	指定なし	1	-
	「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない	1	1
	「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定	1	M※
「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定	指定なし	N※	-
	「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定しない	N※	1
	「表 3-47　複数エントリを使用するフロー検出条件」のパラメータを指定	N※	M※

(凡例)

-：該当なし

N：通常フロー検出条件での使用エントリ数

M：重要フロー検出条件での使用エントリ数

注※　各パラメータで使用するエントリ数を掛け合わせた値

(b) 帯域監視機能でのエントリ数

QoS における帯域監視機能を指定可能なフローリストの最大エントリ数を次の表に示します。

表 3-49　帯域監視機能のエントリ数

モデル	入出力インタフェース当たり		PSU 当たり		装置当たり	
	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33	PSU-1 PSU-12 PSU-43	PSU-2 PSU-22 PSU-33
SB-7804S	4,000	4,000	4,000	4,000	8,000	8,000
SB-7808S					16,000	16,000
SB-7816S					32,000	32,000

なお，通常フロー検出条件，重要パケット保護機能の使用有無，および指定した帯域監視機能によって，1 リストで使用するエントリ数が異なります。

複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-50　複数エントリを使用するフロー検出条件

指定するフロー検出条件	使用エントリ数算出例
VLAN 番号を指定	設定した VLAN 番号数分エントリを使用します。例えば，vlan 1-2 と指定すると，使用エントリ数は 2 となります。 また，vlan と指定した場合の使用エントリ数は，インタフェース名を指定したときは 1 エントリ，物理ポートを指定したときは，指定した物理ポートが所属する VLAN 数となります。
宛先 IPv6 アドレス， 送信元 IPv6 アドレスに pd_prefix を指定	IPv6 DHCP サーバ機能によって，指定したインタフェース名で配布可能な IPv6 プレフィックス数が使用エントリ数となります。 例えば，pd_prefix を指定したインタフェース名に，コンフィグレーション dhcp6_server で，100 個のプレフィックスが割り当てられていた場合，使用エントリ数は 100 となります。

「表 3-51　複数エントリを使用するフロー検出条件」に示したフロー検出条件のパラメータを通常フロー検出条件への指定有無と重要パケット保護機能の使用有無によって，1 リストで使用する帯域監視機能での使用エントリ数が決定します。

なお，「表 3-52　1 リストで使用する帯域監視機能のエントリ数」内 N は，「表 3-51　複数エントリを使用するフロー検出条件」に該当するフロー検出条件の指定方法を二つ以上使用した場合は，各パラメータで使用するエントリ数を掛け合わせた値となり，一つの場合は，そのパラメータで使用するエントリ数となります。

表 3-51　1 リストで使用する帯域監視機能のエントリ数

項番	通常フロー検出条件	重要フロー検出条件	帯域監視設定条件	使用エントリ数
1	「表 3-51　複数エントリを使用するフロー検出条件」の パラメータを指定しない	指定なし	最大帯域制限	1
			最低帯域監視	1
			最大帯域制限＋最低帯域監視	2
2		指定あり	最大帯域制限	2
			最低帯域監視	2

項番	通常フロー検出条件	重要フロー検出条件	帯域監視設定条件	使用エントリ数
			最大帯域制限＋最低帯域監視	4
3	「表 3-51　複数エントリを使用するフロー検出条件」の パラメータを指定	指定なし	最大帯域制限	N※1
			最低帯域監視	N※1
			最大帯域制限＋最低帯域監視	2 × N※1
4		指定あり	最大帯域制限	2 × N※2
			最低帯域監視	2 × N※2
			最大帯域制限＋最低帯域監視	4 × N※2

注※ 1

各パラメータで使用するエントリ数を掛け合わせた値。

注※ 2

pd_prefix は重要パケット保護機能と同時に使用できないため，ここでの N は設定した VLAN 番号数となります。例えば，vlan 1-2 と指定すると，N=2 となります。

（c） ポリシー機能のエントリ数

フィルタにおけるポリシー機能指定可能なフローリストの最大エントリ数は，1,000 エントリです。なお，フロー検出条件によって，1 リストで使用するエントリ数が異なります。1 リストで使用するポリシー機能のエントリ数を次の表に示します。

表 3-52　1 リストで使用するポリシー機能のエントリ数

フロー検出条件	使用エントリ数
VLAN 番号以外を指定	1
VLAN 番号を指定※	N※

注※

指定した VLAN 番号数分エントリを使用します。例えば，vlan 1-2 と指定すると，N=2 となります。

また，VLAN，またはリンクアグリゲーションのインタフェースに対して，ポリシー機能を指定したリストを設定した場合，「1 リストで使用するエントリ数×指定インタフェースがわたる PSU 枚数」分エントリを使用します。例えば，PSU 1,2,3 にわたる VLAN のインタフェースに 1 リストで使用するポリシー機能エントリ数が 10 エントリとなるリストを指定した場合，10 × 3 ＝ 30 エントリを使用します。

（d） NetFlow 統計のエントリ数

NetFlow 統計の最大エントリ数を次の表に示します。

NetFlow 統計のエントリは QoS とエントリを共用します。したがって，NetFlow 統計での使用エントリ数と QoS で使用しているエントリ数の合計が，最大エントリ数を超えた設定はできません。

表 3-53　SB-7804S の収容条件

BCU 搭載メモリ量	装置当たり最大エントリ数		PSU 当たり			
			NetFlow 統計単独使用時の最大エントリ数		NetFlow 統計・QoS の同時使用時の最大エントリ数	
	PSU-1	PSU-2	PSU-1	PSU-2	PSU-1	PSU-2
	PSU-12	PSU-22	PSU-12	PSU-22	PSU-12	PSU-22
	PSU-43	PSU-33	PSU-43	PSU-33	PSU-43	PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000
512MB	16,000	20,000	8,000	16,000	8,000	16,000
768MB	16,000	32,000	8,000	16,000	8,000	16,000
1024MB	16,000	32,000	8,000	16,000	8,000	16,000

表 3-54　SB-7808S の収容条件

BCU 搭載メモリ量	装置当たり最大エントリ数		PSU 当たり			
			NetFlow 統計単独使用時の最大エントリ数		NetFlow 統計・QoS の同時使用時の最大エントリ数	
	PSU-1	PSU-2	PSU-1	PSU-2	PSU-1	PSU-2
	PSU-12	PSU-22	PSU-12	PSU-22	PSU-12	PSU-22
	PSU-43	PSU-33	PSU-43	PSU-33	PSU-43	PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000
512MB	20,000	20,000	8,000	16,000	8,000	16,000
768MB	32,000	50,000	8,000	16,000	8,000	16,000
1024MB	32,000	64,000	8,000	16,000	8,000	16,000

表 3-55　SB-7816S の収容条件

BCU 搭載メモリ量	装置当たり最大エントリ数		PSU 当たり			
			NetFlow 統計単独使用時の最大エントリ数		NetFlow 統計・QoS の同時使用時の最大エントリ数	
	PSU-1	PSU-2	PSU-1	PSU-2	PSU-1	PSU-2
	PSU-12	PSU-22	PSU-12	PSU-22	PSU-12	PSU-22
	PSU-43	PSU-33	PSU-43	PSU-33	PSU-43	PSU-33
256MB	2,000	2,000	2,000	2,000	2,000	2,000
512MB	20,000	20,000	8,000	16,000	8,000	16,000
768MB	50,000	50,000	8,000	16,000	8,000	16,000
1024MB	64,000	100,000	8,000	16,000	8,000	16,000

(20) ダイナミックエントリ，スタティックエントリの最大エントリ数

ダイナミックエントリとスタティックエントリの最大エントリ数を次の表に示します。ダイナミックエントリとスタティックエントリの合計値が，最大装置エントリ数を超えないように使用してください。最大エントリ使用時は「(13) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」に示す搭載メモリ量が必要です。

表 3-56 ダイナミック・スタティック最大エントリ数

項目	最大装置 エントリ数	最大ダイナミック エントリ数	最大スタティック エントリ数
FDB	※	※	※
IPv4 ユニキャスト経路エントリ	45,000/ 装置	45,000/ 装置	4,096/ 装置
IPv4 マルチキャスト経路エントリ	8,000/ 装置	8,000/ 装置	-
IPv6 ユニキャスト経路エントリ	16,384/ 装置	16,384/ 装置	2,048/ 装置
IPv6 マルチキャスト経路エントリ	8,000/ 装置	8,000/ 装置	-
ARP	32,768/ 装置	32,768/ 装置	4,096/ 装置
NDP	8,192/ 装置	8,192/ 装置	1,024/ 装置

(凡例) - : 該当なし

注※

「表 3-14 FDB に登録できる MAC アドレスのエントリ数」を参照してください。

(21) DHCPv6 サーバ (Prefix delegation) の収容条件

DHCPv6 サーバ (Prefix delegation) の最大配布可能 Prefix 数とインタフェース数を次の表に示します。

表 3-57 DHCPv6 サーバ収容条件

項目	最大数
最大配布可能 Prefix 数	8,192 個
インタフェース数	2,048/ 装置

(22) DHCP サーバの収容条件

DHCP サーバの収容条件を次の表に示します。

表 3-58 DHCP サーバ収容条件

項目	最大数
最大配布可能 IP アドレス数	8,192 個
最大固定 IP アドレス割り当て数	320 個
最大インタフェース数	64/ 装置
最大管理サブネット数	64/ 装置

(23) IGMP snooping/MLD snooping の収容条件

IGMP snooping 収容条件を次の表に示します。IGMP snooping で学習したマルチキャスト MAC アドレ

スは FDB に登録します。登録可能なマルチキャスト MAC アドレス数は IGMP snooping と IPv4 マルチキャストを同時に使用する場合に表に示すとおりになります。

表 3-59　IGMP snooping の収容条件

項目	最大数
設定 VLAN 数※1	256(64)
登録エントリ数※2	IPv4 マルチキャストを同時に使用しない：8,000(1,600) IPv4 マルチキャストを同時に使用する　：4,000

注
( ) 内の数値は，BCU の実装メモリが 256MB の場合の最大数です。

注※1
snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4,096(BCU 実装メモリが 256MB の場合は 1,024) です。例えば，各々 20 ポート収容している 128 個の VLAN で snooping を動作させる場合，snooping 動作ポート数は 2,560 となります。

注※2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャスト MAC アドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャスト MAC アドレス分だけエントリを使用します。

MLD snooping 収容条件を次の表に示します。MLD snooping で学習したマルチキャスト MAC アドレスは FDB に登録します。登録可能なマルチキャスト MAC アドレス数は MLD snooping と IPv6 マルチキャストを同時に使用する場合に表に示すとおりになります。

表 3-60　MLD snooping の収容条件

項目	最大数
設定 VLAN 数※1	256(64)
登録エントリ数※2	IPv6 マルチキャストを同時に使用しない：8,000(1,600) IPv6 マルチキャストを同時に使用する　：4,000

注
( ) 内の数値は，BCU の実装メモリが 256MB の場合の最大数です。

注※1
snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4,096(BCU 実装メモリが 256MB の場合は 1,024) です。例えば，各々 20 ポート収容している 128 個の VLAN で snooping を動作させる場合，snooping 動作ポート数は 2,560 となります。

注※2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャスト MAC アドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャスト MAC アドレス分だけエントリを使用します。

(24) IEEE 802.1X

- BCU メモリ

本機能は BCU メモリが 512MByte 以上必要です。もし，BCU メモリが 256MByte で動作させた場合，

本機能および他機能の動作保証はしません。

- 最大認証端末数
  VLAN 単位認証を使用する場合，IEEE 802.1X を設定可能な装置当たりの総ポート数（ポート単位認証の設定されたポート数と VLAN 単位認証の設定された VLAN の持つポート数の合計）は最大 2048 ポートです。この値は 1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば，一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合，その 10 個の VLAN で VLAN 単位認証を動作させせると，総ポート数は 10 ポートになります。本装置の最大認証端末数を次の表に示します。

表 3-61　本装置の最大認証端末数

項目	最大認証端末数
装置当たり	8,192 端末
ポート単位認証当たり	256 端末
VLAN 単位認証（静的）当たり	256 端末
VLAN 単位認証（動的）当たり	8,192 端末

(25) LLDP 機能の収容条件

LLDP 機能では，隣接装置情報の最大収容数は装置当たり 384 です。

(26) OADP 機能の収容条件

OADP 機能では，隣接装置情報の最大収容数は装置当たり 500 です。

3.2.2　SB-5400S の収容条件【**SB-5400S**】

以下に示す条件をすべて満たすようにご使用ください。

(1) BSU の最大テーブルエントリ数

BSU は次に示すテーブルを保有します。

- FDB
- IPv4 ユニキャスト経路（アクティブ経路）
- IPv4 マルチキャスト経路
- ARP
- IPv6 ユニキャスト経路（アクティブ経路）
- IPv6 マルチキャスト経路
- NDP

本装置では，利用形態に合わせ，各テーブルのエントリ数の配分パターンを用意しています。BSU の配分パターンを次の表に示します。なお，表中の「k」の単位は 1,024 です。

表 3-62 BSU のテーブルエントリの配分パターン

想定する利用形態		パターン名	
		l2switch-12	l3switch-12
		L2-SW (IPv4 だけ)	L3-SW (IPv4/IPv6)
L2	FDB	114,688 (112k)	49,152 (48k)
IPv4	ユニキャスト経路※	16,384 (16k)	65,536 (64k)
	マルチキャスト経路	-	8,192 (8k)
	ARP	8,192 (8k)	32,768 (32k)
IPv6	ユニキャスト経路※	-	16,384 (16k)
	マルチキャスト経路	-	8,192 (8k)
	NDP	-	8,192 (8k)

(凡例) - : エントリなし
注※ アクティブ経路

(2) VLAN

VLAN の VLAN 最大数は，ポート当たり 4,080※，装置当たり 4,080※です。また，コンフィグレーションで設定可能な VLAN ID の範囲は，1 ～ 4,095 で，“0”は IEEE802.1Q の仕様上使用できません。

また，“1”はデフォルト VLAN として装置内で使用します。このため，コンフィグレーションによって追加設定が可能な VLAN ID の指定範囲は 2 ～ 4,095 まで定義可能となります。Tag-VLAN 連携を含む通信用の NIF インタフェース数およびトンネルインタフェース数の定義数も，装置当たりの数にカウントします。

本装置で同時に使用可能な VLAN 数は，各ポート上に設定する VLAN 数の全ポート分の合計値に依存します。例えば，192 個のポート上でそれぞれ VLAN を 3 個設定する場合の合計値は，192 × 3 = 576 となります。本装置で同時動作可能な最大の合計値は，25,000 です。この値を超えない範囲で VLAN を設定してください。

注※
VLAN 数（デフォルト VLAN を含む）と Tag-VLAN 連携を含む通信用の NIF のインタフェース，Null インタフェース，トンネルインタフェースの数の合計が 4,080 以内になるようにしてください。

(3) プロトコル VLAN のプロトコル識別数

プロトコル VLAN では，以下のフィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって指定できるプロトコルの種類の最大数はポート当たり 16，装置当たり 16 です。

- EthernetV2 形式フレームの Ether-type 値
- 802.3 形式フレームの LLC 値 (DSAP,SSAP)
- 802.3 形式フレームの Ether-type 値

(4) アップリンク VLAN

VLAN 当たりのアップリンクポートは最大 8 ポートです。

(5) アップリンクブロック

VLAN 当たりのブロックポートは最大 8 ポートです。

(6) プライベート VLAN

Primary VLAN 当たりの Secondary VLAN 数は最大 8 個です。

(7) Tag-VLAN 連携機能

Tag-VLAN 連携機能で使用する Tag-VLAN 数の最大数は，ポート当たり 1,024(Tag なし VLAN を 1 個含む)，装置当たり 1,024 です。

(8) FDB

FDB に登録できる MAC アドレスのエントリの最大数を次の表に示します。FDB の最大エントリ数はコンフィグレーションによって変更できます。「(1) BSU の最大テーブルエントリ数」を参照してください。

なお，1 エントリを装置として運用中に使用することがあるため，実際に FDB として登録できるエントリ数は最大数から 1 減算した値となります。

表 3-63　FDB に登録できる MAC アドレスのエントリ数

モデル	装置当たり最大エントリ数
SB-5402S	114,688 (1,000)
SB-5404S	

注
　( ) 内はその中でスタティックエントリとして登録可能な数です。

(9) リンクアグリゲーション

リンクアグリゲーショングループ当たりの最大ポート数は 16 です。装置当たりのリンクアグリゲーショングループ数は，128 です。

(10) スパニングツリー

PVST+ 数 (VLAN 数と回線数の積) の最大数は，500 です。PVST+ を 100 個の VLAN で動作させ，それぞれの VLAN に 4 回線が所属している場合，PVST+ 数は 100 × 4 = 400 となります。

シングルスパニングツリーを使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，5,000 です。シングルスパニングツリーと PVST+ を併用する場合は，上記 PVST+ 数との合計の最大値が 1,000 となります。

マルチプルスパニングツリーを使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，5,000 です。シングルスパニングツリーまたは PVST+ と併用できません。各 MST インスタンス (MST インスタンス 0 は除く) に対応付けできる VLAN 数の最大数は，50 です。

ただし，VLAN トンネリング機能を使用している場合，各 MST インスタンス (MST インスタンス 0 は除

く) に対応できる VLAN 数の最大数は，装置に実装している物理ポート数に応じて次の表に示すように異なります。表中の全物理回線数とは装置に実装している物理ポート数の総数を指します。なお，CIST に所属する VLAN 数には制限はありません。

表 3-64　各 MST インスタンスに対応できる VLAN 数

全物理回線数	一つの MST インスタンスに設定できる最大 VLAN 数
12 以下	20 以内
24 以下	7 以内
36 以下	5 以内
48 以下	2 以内
96 以下	1 以内
97 以上	0 (CIST だけで運用してください)

（11）GSRP

GSRP でレイヤ 3 冗長切替機能を使用する場合，装置に定義している各 VLAN に設定するポート数の合計 (VLAN 数とポート数の積) の最大数は，5,000 です。

（12）基本制御モジュール (BCU) のメモリ量と収容経路エントリ数

基本制御モジュールのメモリ量と，それに応じた収容可能な IP ユニキャストの経路エントリ数，IP マルチキャストの経路エントリ数，IP インタフェース数，およびフィルタ／ QoS エントリ数を「表 3-66　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，オプションライセンスなし）」～「表 3-73　基本制御モジュールのメモリ量と収容経路エントリ数（オプションライセンス【OP-OSPF(SB-5400S)】あり）」に示します。FDB 数には依存しません。

基本制御モジュールを二重化している場合は，運用系 BCU と待機系 BCU の両方に最小所要メモリ量になるようにメモリ増設が必要です。

経路エントリ数と隣接ルータ数 / 隣接ピア数の関係については，「（16）ルーティングリソース」の収容条件も参照願います。

- 使用する機能によって収容可能な経路エントリ数の条件が変わります。
- OSPF/OSPFv3 を使用する場合は，別途対応するオプションライセンス OP-OSPF が必要です。
- BGP4/BGP4+ を使用する場合は，別途対応するオプションライセンス OP-BGP が必要です。
- IPv4 マルチキャスト /IPv6 マルチキャストを使用する場合は，別途対応するオプションライセンス OP-MLT が必要です。
- IS-IS(IPv4/IPv6) を使用する場合は，別途対応するオプションライセンス OP-ISIS が必要です。
- 最大経路エントリ数のアクティブ数は，以下の式を満たすよう使用して下さい。

  BGP4/BGP4+ OP-BGP を使用しない場合は，以下の式から BGP4/BGP4+ を外して考えます。

  IPv4 の場合

  アクティブ数 ≧ (RIP+OSPF+IS-IS，BGP4，スタティックを合わせたアクティブ経路数)
  ＋ IPv4 インタフェース数× 2 (直結経路 (ホスト経路とサブネット経路))
  かつ
  「表 3-63　BSU のテーブルエントリの配分パターン」の配分パターンの IPv4 ユニキャストエントリ経路数に関し
  IPv4 ユニキャストエントリ経路数 ≧

アクティブ数 ＋ ARP エントリ数 ＋ IPv4 インタフェース数× 2 ＋ 3

IPv6 の場合

アクティブ数 ≧ (RIPng+OSPFv3+IS-IS，BGP4+，スタティックを合わせたアクティブ経路数）
＋ IPv6 インタフェース数× 2
(直結経路のグローバルアドレス (ホスト経路とネットワーク経路))
かつ
「表 3-63　BSU のテーブルエントリの配分パターン」の配分パターンの IPv6 ユニキャストエントリ経路数に関し
IPv6 ユニキャストエントリ経路数 ≧
アクティブ数 ＋ NDP エントリ数 ＋ IPv6 インタフェース数× 3
(直結経路のリンクローカルアドレス (ホスト経路とネットワーク経路) とリンクローカルマルチキャストアドレス一つ)

- 特に注がない場合はマルチパス数は 4 です。
- 最大経路エントリ数には，スタティック経路，ダイレクト経路，集約経路，デフォルト経路，およびループバック経路を含みます。
- NetFlow 統計は QoS とエントリを共用します。したがって，NetFlow 統計で使用しているエントリ数と QoS で使用しているエントリ数の合計が，QoS エントリの最大数を超えた設定はできません。

[表の見方]

表の項目に記載の経路エントリ数は，「基本制御モジュールのメモリ量に応じた収容可能な」IP ユニキャストの経路エントリ数，IP マルチキャストの経路エントリ数，IP インタフェース数，およびフィルタ／ QoS エントリ数を示します。
インタフェース数で IPv4/IPv6 インタフェース数と記載のある場合，インタフェース数は IPv4 と IPv6 インタフェース数の合計値の最大値を示します。
また，IPv4/IPv6 インタフェース数と記載のインタフェースの最大数については，IPv4 と IPv6 で独立に数え，値が 1,024 であれば，IPv4 のアドレスを設定したインタフェースの最大値が 1,024，IPv6 のアドレスを設定したインタフェースの最大値が 1,024 を意味します。例えば，IPv4 だけを使用した場合は，インタフェースの最大値が 1,024 となります。IPv6 だけを使用した場合は，インタフェースの最大値が 512 となります。IPv4 と IPv6 を混在した場合は，IPv4 と IPv6 インタフェース数の合計値の最大値を示します。基本制御モジュールを二重化している場合は，運用系 BCU と待機系 BCU の両方に最小所要メモリ量になるようメモリ増設が必要です。
なお，「表 3-66　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，オプションライセンスなし）」～「表 3-73　基本制御モジュールのメモリ量と収容経路エントリ数（オプションライセンス【OP-OSPF(SB-5400S)】あり）」の注意事項は，「表 3-73　基本制御モジュールのメモリ量と収容経路エントリ数（オプションライセンス【OP-OSPF(SB-5400S)】あり）」の後ろにまとめて記述しています。

(a) l3switch-12 のテーブルエントリ数の配分パターン

● IPv4 のルーティングプロトコルだけ (RIP だけ) を使用する場合

表 3-65 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけを使用し，オプションライセンスなし）

BCU 最小所要メモリ量	IPv4 ユニキャスト						フィルタ / QoS エントリ数※8	PVST+ 数
	最大経路エントリ数		プロトコル別最大経路エントリ数		ARP エントリ数	インタフェース数※6		
	アクティブ／非アクティブの合計	アクティブ	RIP	スタティック				
256MB ※9	1,768	1,768	1,000	512	8,192	256	2,000	128
512MB	3,768	3,768		2,048			8,000	500
768MB								
1024MB								

● IPv4 のルーティングプロトコルだけ (オプションライセンス**【OP-OSPF(SB-5400S)】【OP-BGP】【OP-MLT】【OP-ISIS】**のどれかあり) の場合

表 3-66 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4 だけ使用し，オプションライセンスあり）

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト		IPv4 インタフェース数	フィルタ /QoS エントリ数※8	PVST + 数
	最大経路エントリ数		プロトコル別最大経路エントリ数			ARP エントリ数	PIM-SM/SSM ※3				
	アクティブ／非アクティブの合計	アクティブ	RIP ※7 +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※3			
256MB ※9	※5										
	3,768	3,768	3,000	-	256	8,192	-	-	256	2,000	128
			2,500		512						
512MB	45,000	45,000	30,000	45,000	2,048		※2		1,024 ※4	8,000	500
768MB											
1024MB											

(凡例) - : 適用しない

● IPv4/IPv6 のルーティングプロトコル (RIP/RIPng だけ) を使用する場合

基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスなし）の表の (1/2) と (2/2) を次に示します。

表 3-67 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスなし）(1/2)

BCU 最小所要メモリ量	IPv4 ユニキャスト				
	最大経路エントリ数		プロトコル別 最大経路エントリ数		ARP エントリ数
	アクティブ／非アクティブの合計	アクティブ	RIP	スタティック	
256MB※9	1,768	1,768	1,000	512	8,192
512MB	3,768	3,768		2,048	
768MB					
1024MB					

表 3-68 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスなし）(2/2)

BCU 最小所要メモリ量	IPv6 ユニキャスト					IPv4/IPv6 インタフェース数※6	フィルタ / QoS エントリ数※8	PVST+ 数
	最大経路エントリ数		プロトコル別 最大経路エントリ数		NDP エントリ数			
	アクティブ／非アクティブの合計	アクティブ	RIPng	スタティック				
256MB※9	1,768	1,768	1,000	512	4,096	256	2,000	128
512MB	3,768	3,768		2,048			8,000	500
768MB								
1024MB								

● **IPv4/IPv6 のルーティングプロトコル (オプションライセンス【OP-OSPF(SB-5400S)】【OP-BGP】【OP-MLT】【OP-ISIS】のどれかあり) の場合**

基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスあり）の表の (1/2) と (2/2) を次に示します。

表 3-69 基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスあり）（1/2）

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト	
	最大経路エントリ数		プロトコル別 最大経路エントリ数			ARP エントリ数	PIM-SM/SSM	
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※3
256MB※9	※5							

BCU 最小所要メモリ量	IPv4 ユニキャスト						IPv4 マルチキャスト	
	最大経路エントリ数		プロトコル別最大経路エントリ数			ARP エントリ数	PIM-SM/SSM	
	アクティブ／非アクティブの合計	アクティブ	RIP +OSPF +IS-IS	BGP4	スタティック		(S,G) エントリ数	インタフェース数※3
	3,768	3,768	3,000	-	256	8,192	-	-
			2,500		512			
	1,768	1,768	1,000					
512MB	45,000	45,000	30,000	45,000	2,048		※2	
768MB								
1024MB								

（凡例）　-：該当なし

表 3-70　基本制御モジュールのメモリ量と収容経路エントリ数（IPv4/IPv6 を使用し，オプションライセンスあり）(2/2)

BCU 最小所要メモリ量	IPv6 ユニキャスト						IPv6 マルチキャスト		IPv4/IPv6 インタフェース数※6	フィルタ / QoS エントリ数※8	PVST+ 数
	最大経路エントリ数		プロトコル別最大経路エントリ数			NDP エントリ数	PIM-SM/SSM				
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPFv3 +IS-IS	BGP4+	スタティック		(S,G) エントリ数	インタフェース数※3			
256MB ※9	※5										
	-	-	-	-	-	-	-	-	256	2,000	128
	1,768	1,768	1,000		512	4,096					
512MB	16,384	16,384	10,000	16,384	2,048	8,192	※2		1,024	8,000	500
768MB									※4		
1024MB											

（凡例）　-：該当なし

（b） l2switch-12 の配分パターンの場合

● IPv4 のルーティングプロトコル (RIP だけ) を使用する場合

表 3-71　基本制御モジュールのメモリ量と収容経路エントリ数（オプションライセンスなし）

BCU 最小所要メモリ量	IPv4 ユニキャスト						フィルタ / QoS エントリ数※8	PVST+ 数
	最大経路エントリ数		プロトコル別 最大経路エントリ数		ARP エントリ数	インタフェース数※6		
	アクティブ／非アクティブの合計	アクティブ	RIP	スタティック				
256MB ※9	1,768	1,768	1,000	512	8,192	256	2,000	128
512MB	3,768	3,768		2,048			8,000	500
768MB								
1024MB								

● IPv4 のルーティングプロトコル (オプションライセンス【**OP-OSPF(SB-5400S)**】) を使用する場合

表 3-72　基本制御モジュールのメモリ量と収容経路エントリ数（オプションライセンス【**OP-OSPF(SB-5400S)**】あり）

BCU 最小所要メモリ量	IPv4 ユニキャスト					IPv4 インタフェース数※6	フィルタ /QoS エントリ数※8	PVST+ 総回線数
	最大経路エントリ数		プロトコル別 最大経路エントリ数		ARP エントリ数			
	アクティブ／非アクティブの合計	アクティブ	RIP※7 +OSPF +IS-IS	スタティック				
256MB ※9	3,768	3,768	3,000	256	8,192	256	2,000	128
			2,500	512				
512MB, 768MB, 1024MB			3,000	256			8,000	500
			2,500	512				

注※ 1

PIM-SM/SSM と PIM-DM は，同時に動作できません。(注※ 2) に示す (S，G) エントリ数とインタフェース数の組み合わせで使用するメモリ量は PIM-SM/SSM と PIM-DM は同じです。

注※ 2

(S，G) エントリ数とインタフェース数の組み合わせは，以下のどれかの組み合わせでご使用ください。

表 3-73　（S,G）エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
8,000	32
5,000	64
3,000	128

注※ 3

PIM-SM/SSM の場合，使用可能なインタフェース数は，表中の (数値 -1) です。32 であれば 31 までです。また，このインタフェース数はコンフィグレーションコマンド (pim コマンド max-interfaces サブコマンド /pim6 コマンド max-interfaces サブコマンド) により指定してください。指定しない場合のデフォルト値は 128 です。

注※ 4

IPv6 の最大インタフェース数は，512 です。

注※ 5

IPv4 ユニキャスト，IPv4 マルチキャスト，IPv6 ユニキャスト，IPv6 マルチキャスト，ARP，NDP，フィルタ / QoS，インタフェース数，PVST+ 数は最小値であれば，同時に動作可能です。

注※ 6

VLAN 定義に関しては IP 定義の有無に関わらず，IP インタフェースを消費します。

注※ 7

RIP または RIPng の最大経路エントリ数は 1,000 までです。

注※ 8

NetFlow 統計は QoS とエントリを共用します。したがって，NetFlow 統計で使用しているエントリ数と QoS で使用しているエントリ数の合計が，QoS エントリの最大数を超えた設定はできません。

注※ 9

256MB を搭載する場合は下記をご注意ください。

記載されている各機能のすべてのエントリ数の収容で，オンラインによる下記のコンフィグレーションの追加／削除／変更を実施する場合は搭載メモリを 512MB 以上で運用してください。

1. 装置管理情報
2. SNMP 情報
3. 回線（Line）情報
4. トンネル情報
5. レイヤ 2 スイッチ情報
6. IP インタフェース情報
7. IP ルーティングプロトコル情報
8. IP マルチキャストルーティングプロトコル情報
9. フロー情報
10. QoS 情報
11. デフォルト情報
12. VRRP 情報
13. RA 情報
14. ホスト名情報
15. ログ情報
16. NTP 情報
17. Disable 情報

（13）インタフェース数

IPv4 アドレス，および IPv6 アドレスを付与する単位をインタフェースと呼びます。そのインタフェース数の最大値は，装置当たり 1,024 です。IPv4 と IPv6 インタフェース数は独立して数え，IPv4 と IPv6 のインタフェース数の合計値が最大インタフェース数を超えないように使用してください。この値に含むインタフェースは，Tag-VLAN 連携を含む通信用の NIF のインタフェース，VLAN インタフェース，Null インタフェース，トンネルインタフェースを含みます。リモートマネージメントポートのインタフェースの数は含みません。また，最大インタフェース数での動作はスタティックルートを前提にしています。RIP,OSPF などのダイナミックルーティングの場合は，経路計算性能によって実効的な最大インタフェース数が制限されます。

(a) 最大トンネルインタフェース数

IPv6 over IPv4 トンネルインタフェース数は，装置当たり最大 256 です。IPv4 over IPv6 トンネルインタフェース数は，装置当たり最大 256 です。6to4 トンネルインタフェース数は，装置当たり最大 1 です。また，IPv6 over IPv4 トンネル，IPv4 over IPv6 トンネル，および 6to4 トンネルのインタフェース数の合計値は，装置当たり最大 256 です。

(14) アドレス数

コンフィグレーションで設定できる IPv4 アドレスの最大数は，1,024 です。この値は，マルチホーム，Tag-VLAN 連携を含む通信用の NIF のインタフェース，VLAN インタフェースおよびトンネルインタフェースに設定できる IPv4 アドレス数です。リモートマネージメントポートに設定できる IPv4 アドレス数は含みません。

また，コンフィグレーションで設定できる IPv6 アドレスの最大数は，512 です。この値は，マルチホーム，Tag-VLAN 連携を含む通信用の NIF のインタフェースおよびトンネルインタフェースに設定できる IPv6 アドレス数です。

(a) マルチホームの最大アドレス数

LAN のマルチホーム接続では一つのインタフェースに対して，複数の IPv4 アドレス，または IPv6 アドレスを設定できます。

マルチホーム接続においてコンフィグレーションで設定できる IPv4 最大アドレス数は，インタフェース当たり最大 256，IPv6 最大アドレス数は，インタフェース当たり最大 7 です。

なお，IPv6 の場合，一つのインタフェースには必ず一つのリンクローカルアドレスが設定されるため，マルチホーム接続でインタフェースに IPv6 グローバルアドレスだけ定義した場合，実際に装置に設定される IPv6 アドレス数は，自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 となります。

(15) 最大相手装置数

本装置が直接収容する LAN を介して IP 通信できる最大相手装置数を示します。この場合の相手装置はルータに限らず端末も含みます。

(a) ARP エントリ数，NDP エントリ数

イーサネットでは，ARP，NDP などのアドレス解決によって，送信しようとするパケットの宛先 IP アドレスに対応するハードウェアアドレスを決定します。したがって，ARP エントリ数，NDP エントリ数によって最大相手装置数が決まります。ARP エントリ数，NDP エントリ数を次の表に示します。

表 3-74 ARP エントリ数，NDP エントリ数

項目	最大エントリ数（装置当たり）
ARP	32,768
NDP	8,192

注 1

ダイナミックエントリとスタティックエントリの最大エントリ数については，「表 3-99 ダイナミック・スタティック最大エントリ数」を参照してください。

注 2

全エントリを 1 インタフェースで使用することもできます。

注 3

ARP と NDP は独立動作です。それぞれ最大エントリ数を使用できます。

(b) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 3-75 RA の相手端末数

項目	最大相手端末数
RA	1,024

注

相手端末数に応じて RA の送信間隔は制限されます。詳細は,「コンフィグレーションコマンドレファレンス Vol.1 11. RA 情報」のコンフィグレーションコマンド ra を参照してください。

(16) ルーティングリソース

(a) 最大隣接ルータ数

最大隣接ルータ数を「表 3-77 最大隣接ルータ数」に示します。最大隣接ルータ数の定義はルーティングプロトコルによって異なります。各プロトコルの最大隣接ルータ数の定義を「表 3-79 最大隣接ルータ数の定義」に示します。

表 3-76 最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数
スタティックルーティング (IPv4,IPv6 の合計)	2,048※
OSPF	150
OSPFv3	50
IS-IS	25
RIP,OSPF,BGP4,RIPng,OSPFv3,BGP4+,IS-IS の合計	256

注※

動的監視機能を使用する隣接ルータは,ポーリング間隔によって数が制限されます。詳細は,次の表のスタティックの動的監視機能を使用できる最大隣接ルータ数を参照してください。

表 3-77 スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
5 秒	300
10 秒	600
20 秒	1,200

表 3-78 最大隣接ルータ数の定義

ルーティングプロトコル	定義
スタティックルーティング	ネクストホップ・アドレスの数
RIP	RIP が動作するインタフェース数
RIPng	RIPng が動作するインタフェース数

ルーティングプロトコル	定義
OSPF	OSPF が動作する各インタフェースにおける下記の総計 1. 該当するインタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当するインタフェースと接続されるほかの OSPF ルータの数 2. 該当するインタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当するインタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンドの show ip ospf neighbor コマンドで表示される隣接ルータの状態（State）が「Full」となる隣接ルータの数と同じ意味になります。
OSPFv3	OSPFv3 が動作する各インタフェースにおける下記の総計 1. 該当するインタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当するインタフェースと接続されるほかの OSPFv3 ルータの数 2. 該当するインタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当するインタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンドの show ipv6 ospf neighbor コマンドで表示される隣接ルータの状態（State）が「Full」となる隣接ルータの数と同じ意味になります。
BGP4	BGP4 ピア数
BGP4+	BGP4+ ピア数
IS-IS	本装置と接続されるほかの IS-IS ルータの数

注

コンフィグレーションのインタフェースパラメータを省略した場合はすべてのインタフェースが対象になります。

(b) 経路エントリ数と最大隣接ルータ数の関係

経路エントリ数と最大隣接ルータ数（RIP/RIPng，OSPF/OSPFv3，IS-IS)，経路エントリ数と最大ピア数 (BGP,BGP4+) の関係を「表 3-80　経路エントリ数と最大隣接ルータ数の関係」～「表 3-82　経路エントリ数と最大ピア数の関係 (IPv4，IPv6 混在)【OP-BGP】」に示します。

なお，最大隣接ルータ数は本装置より経路広告を行うルータ数となります。

表 3-79　経路エントリ数と最大隣接ルータ数の関係

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数	備考
RIP	1,000	100	※2
RIPng	1,000	100	
OSPF※3	1,000	150	
	2,000	75	
	5,000	30	
	10,000	15	
OSPFv3※3	1,000	50	
	2,000	25	
	5,000	10	
	10,000	5	
IS-IS※4	1,000	25	
	2,000	12	
	5,000	5	
	10,000	2	

注※1

最大経路エントリ数は代替経路を含みます。

注※2

各ルーティングプロトコル (RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+) を併用して使用する場合の最大隣接ルータ数は，各々 1/n(n : 使用ルーティングプロトコル数) となります。例えば，BGP，BGP4+ を使用せず，OSPF(5,000 経路) と OSPFv3(5,000 経路) を併用して使用する場合の最大隣接ルータ数は，1/2 である，OSPF では 15，OSPFv3 では 5 となります。

注※3

OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※4

IS-IS の最大経路エントリ数は，IPv4 経路エントリ数と IPv6 経路エントリ数の合計とします。

表 3-80　経路エントリ数と最大ピア数の関係（IPv4 だけ）【OP-BGP】

ルーティングプロトコル	上位ピア数※1	BCU の実装メモリ	最大経路エントリ	最大隣接ピア数 ※2※3※4※5
BGP4	2	512MB	22,500	256
		768MB	22,500	256
		1024MB	22,500	256
	3	512MB	15,000	256
		768MB	15,000	256
		1024MB	15,000	256
	4	512MB	11,250	256
		768MB	11,250	256
		1024MB	11,250	256

表 3-81 経路エントリ数と最大ピア数の関係 (IPv4，IPv6 混在)【OP-BGP】

ルーティングプロトコル	上位ピア数※1	BCU の実装メモリ	最大経路エントリ		最大隣接ピア数 ※2※3※4※5
			IPv4	IPv6	
BGP4 BGP4+	2	512MB	22,500	8,192	128
		768MB	22,500	8,192	128
		1024MB	22,500	8,192	128
	3	512MB	15,000	5,460	64
		768MB	15,000	5,460	128
		1024MB	15,000	5,460	128
	4	512MB	11,250	4,096	32
		768MB	11,250	4,096	128
		1024MB	11,250	4,096	128

注※ 1
上位ピア数とは，最大経路エントリ数を広告してくるピアの数を示します。

注※ 2
最大隣接ピア数とは，上位ピアから受信した経路を広告するピアの数を示します。表に示す値はマルチキャスト未使用で，かつマルチパス数が 4，送受信フィルタリングによる属性変更なしの場合の値です。

注※ 3
BGP4 と BGP4+ は独立動作です。BGP4 と BGP4+ それぞれでこの表に示す最大隣接ピア数を使用できます。

注※ 4
「最大隣接ピア数 =0」は「上位ピアからの BGP 経路を受け取ることはできるが，隣接ピアに広告することはできない」ことを意味します。

注※ 5
「最大隣接ピア数 = ×」は「上位ピアからの BGP 経路を受け取ることができない」ことを意味します。

(17) IPv4/IPv6 マルチキャスト【OP-MLT】

IPv4/IPv6 マルチキャスト定義できるインタフェース数およびマルチキャスト経路情報のエントリ数を次の表に示します。マルチキャスト経路情報のエントリ数とインタフェース数によって必要となる搭載メモリ量が異なります。

本装置は IPv4 マルチキャストルーティングプロトコルとして PIM-SM，PIM-SSM，PIM-DM および DVMRP をサポートします。ただし，PIM-SM と PIM-SSM 以外のプロトコルは同時には動作しません。IPv6 マルチキャストルーティングプロトコルとして PIM-SM，および PIM-SSM をサポートします。

IPv4 マルチキャストと IPv6 マルチキャストは同時に動作でき，かつ PIM-SM と PIM-SSM は同時に動作できます。

表 3-82 IPv4/IPv6 マルチキャストの最大数

項目	IPv4 最大数	IPv6 最大数
PIM-SM/SSM マルチキャストインタフェース数	127 ／装置※1※2	127 ／装置※3※4
IGMP/MLD 動作インタフェース数	128 ／装置※5	127 ／装置※3
1 グループ当たりの送信元数	256 ／グループ	256 ／グループ

項目	IPv4 最大数	IPv6 最大数
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ，(*,G) エントリ，およびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	8,000 ／装置	8,000 ／装置
PIM-DM/DVMRP マルチキャスト経路情報のエントリ ((S,G) エントリおよびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	8,000 ／装置	-
IGMPv2/IGMPv3(EXCLUDE モード) / MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連携動作させる設定数	256 ／装置※ 6	256 ／装置※ 7
IGMPv3/MLDv2 における Report 内に格納できるグループ情報	32 record ／メッセージ 32 ソース／ record	32 record ／メッセージ※ 8 32 ソース／ record
IGMP/ MLD 加入グループ数※ 9	IGMP 256 ／装置※ 10	MLD 256 ／装置※ 10
マルチキャストルータ隣接数	128 ／装置	128 ／装置
ランデブーポイント数	1 ／グループ	1 ／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128 ／装置	128 ／装置
1 システム当たりランデブーポイントで設定できる延べグループ数	128 ／システム	128 ／システム
BSR 候補数	1 ／システム	1 ／システム
1 インタフェース当たりの静的グループ加入数	256 ／インタフェース	256 ／インタフェース
静的グループ加入数※ 11	8,192 ／装置※ 12	8,192 ／装置
静的ランデブーポイントルータアドレス数	16 ／装置	16 ／装置
IGMP/ MLD グループ当たりのソース数	256 ／グループ	256 ／グループ
(S,G) エントリ当たりの出力物理ポート延べ数 ※ 13	384 ／エントリ	384 ／エントリ
PIM-DM マルチキャストインタフェース数	128 ／装置※ 1	-
DVMRP マルチキャストインタフェース数	16 ／装置※ 1 ※ 14	-

(凡例) - : 該当なし

注※ 1

マルチホームはサポートしていません。

注※ 2

PIM-SM インタフェースと PIM-SSM インタフェースの合計で 127/ 装置です。

注※ 3

マルチホームもサポートしています。

注※ 4

IPv6 マルチキャストインタフェースとして，このほかにカプセル化用インタフェースが一つ存在します。このため，IPv6 PIM-SM マルチキャストインタフェース全体の数は 128 個になりますが，ユーザが設定できるのはそのうち 127 個です。また，PIM-SM と PIM-SSM の合計で 128 個となります。

注※ 5

使用するマルチキャストルーティングプロトコルによって異なります。

- PIM-SM/PIM-SSM：127
- PIM-DM：128
- DVMRP：16

注※ 6

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-84　使用インタフェース数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-85　加入グループ数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。

表 3-83　使用インタフェース数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256

表 3-84　加入グループ数に対する IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数（のべ数）	IGMPv1/IGMPv2/IGMPv3(EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1,024	16
2,048	8
4,096	3
8,192	1

加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つでなく，加入したインタフェースの数になります。一つの IGMPv3（EXCLUDE モード）Report で PIM-SSM を連携動作させる設定数は 256 になります。例えば，一つの IGMPv3（EXCLUDE モード）Report 内に三つの record があり，各 record に対応する PIM-SSM を連携動作させる設定数の合計が 256 を超えた場合，以降の record に対する本設定は無視します。

注※ 7

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-86　使用インタフェース数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-87　加入グループ数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。

表 3-85 使用インタフェース数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256

表 3-86 加入グループ数に対する MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数（のべ数）	MLDv1/MLDv2(EXCLUDE モード) で PIM-SSM を連動させる設定数
32	256
64	128
128	64
256	32
512	16
1,024	8
2,048	4
4,096	2
8,192	1

加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つでなく，加入したインタフェースの数になります。一つの MLDv2（EXCLUDE モード）Report で PIM-SSM を連携動作させる設定数は 256 になります。例えば，一つの MLDv2（EXCLUDE モード）Report 内に三つの record があり，各 record に対応する PIM-SSM を連携動作させる設定数の合計が 256 を超えた場合，以降の record に対する本設定は無視します。

注※ 8

一つの Report メッセージで処理できるソース数は延べ 1,024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

MLDv2 での EXCLUDE モードで SSM に接続する設定をした場合，受信した Report メッセージ内の record のソース数がのべ 1,024 を超えた以降の record は無視します。

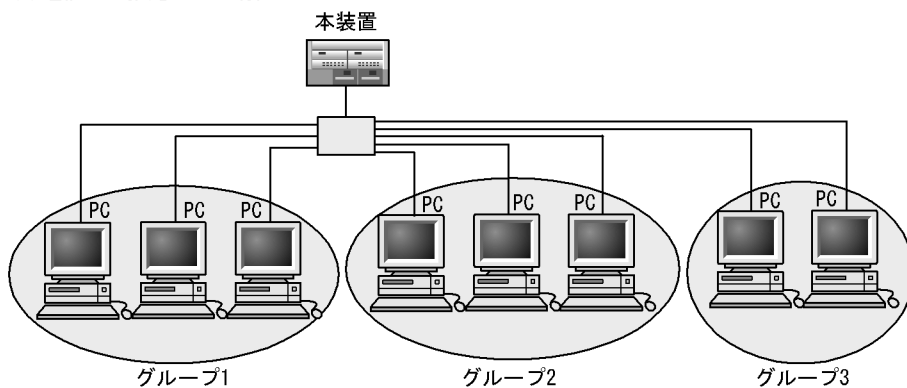
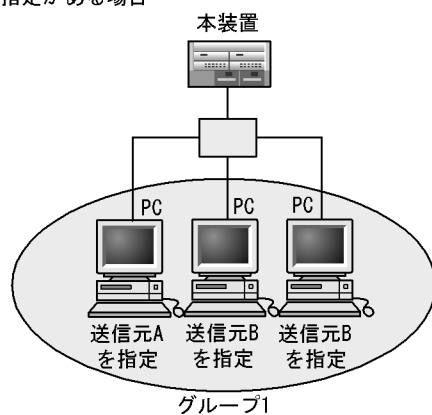
例えば，MLDv2EXCLUDE モードで SSM に接続する設定をマスク指定で 1 グループに対し 256 ソースの定義をした場合，次のようになります。

1. 受信した MLDv2 Report メッセージ内の先頭からこの設定に一致する二つの EXCLUDE の record が存在した場合，5record 目以降を無視します。
2. 受信した MLDv2 Report メッセージ内に 1 ソースの INCLUDE の record があり，この設定に一致するグループの EXCLUDE が 4record あった場合，4record 目以降から無視します。

注※ 9

本装置に直接接続しているグループの数です。IGMPv3/MLDv2 使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。

次の図の (1) の例では 3 です。(2) の例では (送信元 A，グループ 1) および (送信元 B，グループ 1) の組み合わせになるため，グループ数は 2 になります。

図 3-2　マルチキャストグループ数の例

注※ 10

IPv4 におけるインタフェース当たりの加入可能グループ数を次の表に示します。

表 3-87　IPv4 におけるインタフェース当たりの加入グループ数

マルチキャスト 動作インタフェース数	インタフェース当たりの加入可能グループ数 （グループ＋ソース数）
31	256
63	128
127	64

IPv6 におけるインタフェース当たりの加入可能グループ数を次の表に示します。

表 3-88　IPv6 におけるインタフェース当たりの加入可能グループ数

マルチキャスト 動作インタフェース数	インタフェース当たりの加入可能グループ数 （グループ＋ソース数）
31	256
63	128
127	64

注※ 11

静的グループ加入数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総計

です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的グループ加入数は一つではなく，静的加入設定したインタフェースの数となります。

注※ 12
PIM-DM または DVMRP は 64/ 装置です。

注※ 13
(S,G) エントリの出力インタフェースが VLAN の場合，1 出力インタフェースに対して物理ポートが複数になる場合があります。この場合の出力物理ポート延べ数は，各出力インタフェースに対する物理ポートの総数となります。
例えば，出力インタフェース数が 2 で，インタフェース当たりの物理ポート数が 5 の場合，出力物理ポート延べ数は 10 となります。

注※ 14
DVMRP を使用する場合は，本装置の全インタフェース数を 500 以下の環境で使用してください。

(a) PIM-SM ／ PIM-SSM ／ PIM-DM 使用時の注意

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

マルチキャストデータの送信元となるサーバの中には，マルチキャストパケットをバーストトラフィックとして送信する特性を持つものがあります。この特性を持つサーバから受信したマルチキャストデータを，マルチキャスト配信する場合には注意が必要です。マルチキャスト配信先の回線を収容するネットワークインタフェースモジュール（NIF）の種類によって，マルチキャスト動作可能なインタフェース数が異なります。マルチキャスト動作可能なインタフェース数を次の表に示します。

表 3-89 マルチキャスト動作可能なインタフェース数（ポート当たり，NIF 当たり）

NIF 略称	マルチキャスト動作可能なインタフェース数（推奨値※）
NF100-48TA	8 ポート当たり 8 インタフェース
NF1G-6G	ポート当たり 8 インタフェース
NF1G-32S	8 ポート当たり 8 インタフェース
NF1G-48T	8 ポート当たり 8 インタフェース
NFMX-44	• 10/100/1000BASE-T の 8 ポート当たり 8 インタフェース • 1000BASE-X の 4 ポート当たり 8 インタフェース
NFMX-34	• 10/100/1000BASE-T の 8 ポート当たり 8 インタフェース • 選択型 10/100/1000BASE-T /1000BASE-X のポート当たり 8 インタフェース

注※
推奨値は，送信元サーバが，マルチキャストパケットを 8 バーストで送信する特性（サーバで 8 パケット分のマルチキャストデータをいったん蓄積した後に，ネットワークに対して連続的に送信する特性）を持っていることを想定しています。バースト数が大きくなると，パケットを一部廃棄することがあるので，マルチキャスト定義するインタフェース数を少なくする必要があります。

(18) フィルタリング・QoS

ここでのエントリ数とは，コンフィグレーションで設定した内容を装置内部で使用する形式 (エントリ) に変換した後の数です。

(a) フィルタ /QoS エントリ数

フィルタおよび QoS のエントリ数を次の表に示します。

表 3-90 フィルタ /QoS エントリ数（装置当たり）

BCU 搭載メモリ量	フィルタ・QoS 同時使用時の装置当たりの最大エントリ数 (フィルタと QoS エントリの合計)	フィルタ単独使用時の装置当たりの最大エントリ数	QoS 単独使用時の装置当たりの最大エントリ数
256MB	2,000	2,000	2,000
512MB	8,000	4,000	4,000
768MB	8,000	4,000	4,000
1024MB	8,000	4,000	4,000

フローフィルタ情報およびフロー QoS 情報はフローコンフィグレーションで定義しますが，リストに設定するフロー検出条件パラメータによって使用するエントリ数が異なります。

複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-91 複数エントリを使用するフロー検出条件

複数エントリを使用するフロー検出条件のパラメータの指定	使用エントリ数算出例
宛先 IPv4 アドレス， 送信元 IPv4 アドレス， 宛先 IPv6 アドレス， 送信元 IPv6 アドレス を範囲指定	指定された IP アドレスが幾つのサブネットに区切られるかによって使用エントリ数が決定します。 例えば，宛先 IPv4 アドレスに 192.168.0.1-192.168.0.4 と指定した場合， 192.168.0.1/32, 192.168.0.2/31, 192.168.0.4/32 の三つのサブネットに区切られますので，使用エントリ数は 3 となります。 そのほかも同様です。
宛先 IPv6 アドレス， 送信元 IPv6 アドレスに pd_prefix を指定	IPv6 DHCP サーバ機能によって，指定したインタフェース名で配布可能な IPv6 プレフィックス数が使用エントリ数となります。 例えば，pd_prefix を指定したインタフェース名に，コンフィグレーション dhcp6_server で，100 個のプレフィックスが割り当てられていた場合，使用エントリ数は 100 となります。
宛先ポート番号を範囲指定， 送信元ポート番号を範囲指定， IP ユーザデータ長上限値， IP ユーザデータ長下限値	指定された値が最大 16 ビットのマスクで区切ったときに幾つに分けられるかによって使用エントリ数が決定します。 例えば，宛先ポート番号に 135-140 と指定した場合， 135/16 = 0000 0000 1000 0111(2 進表記) 136/14 = 0000 0000 1000 10xx(2 進表記) 140/16 = 0000 0000 1000 1100(2 進表記) の三つの領域に区切られますので，使用エントリ数は 3 となります。 そのほかも同様です。 なお，IP ユーザデータ長上限値指定時は，0 〜 (指定上限値 +20 バイト※1) ※2 の範囲指定となります。また，IP ユーザデータ長下限値指定時は，(指定下限値 +20 バイト※1) 〜 65,535 までの範囲指定となります。
VLAN 番号を複数指定	設定した VLAN 番号数分エントリを使用します。例えば，vlan 1-2 と指定すると，使用エントリ数は 2 となります。 また，vlan と指定した場合の使用エントリ数は，インタフェース名を指定したときは 1 エントリ，物理ポートを指定したときは，指定した物理ポートが所属する VLAN 数となります。

注※ 1

IP ヘッダ長 20 バイト分を指定値に足して計算を行います。

注※ 2

「指定上限値 + IP ヘッダ長 20 バイト」が 65,535 より大きい場合は，0 〜 65,535 の範囲指定となります。

● フィルタ，QoS 機能での 1 リストで使用するエントリ数

1 リストで使用するエントリ数は次のとおりです。

- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを一つ指定した場合，指定したパラメータで使用するエントリ数が，1 リストで使用するエントリ数（「表 3-93　1 リストで使用するエントリ数 (フィルタ)」の N）となります。
- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを二つ以上指定した場合，各パラメータで使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数（「表 3-93　1 リストで使用するエントリ数 (フィルタ)」の N）となります。
  例えば，1 リストに宛先 IPv4 アドレスの範囲指定と送信元 IPv4 アドレスの範囲指定を指定した場合，「1 リストで使用するエントリ数（「表 3-93　1 リストで使用するエントリ数 (フィルタ)」の N）= 宛先 IPv4 アドレスの範囲指定での使用エントリ数×送信元 IPv4 アドレスの範囲指定での使用エントリ数」となります。
- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを指定しない場合，使用エントリ数は 1 エントリとなります。

表 3-92　1 リストで使用するエントリ数 (フィルタ)

設定条件	使用エントリ数
「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを指定しない	1
「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを指定	N ※

注※　各パラメータで使用するエントリ数を掛け合わせた値

● QoS 機能における 1 リストで使用するエントリ数

1 リストで使用するエントリ数は，重要パケット保護機能を指定した場合，「通常フロー検出条件で使用するエントリ数＋重要フロー検出条件で使用するエントリ数」となります。重要パケット保護機能を使用しない場合は，通常フロー検出条件で使用するエントリ数が，1 リストで使用するエントリ数となります。

通常・重要フロー検出条件で使用するエントリ数は，次のとおりです。

- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを一つ指定した場合，指定したパラメータで使用するエントリ数が 1 リストで使用するエントリ数（「表 3-94　1 リストで使用するエントリ数（QoS)」）となります。
- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを二つ以上指定した場合，各パラメータで使用するエントリ数（「表 3-94　1 リストで使用するエントリ数（QoS)」）を掛け合わせた値となります。
- 「表 3-92　複数エントリを使用するフロー検出条件」のパラメータを指定しない場合，使用エントリ数は 1 エントリとなります。

表 3-93 1 リストで使用するエントリ数（QoS）

通常フロー検出条件	重要フロー検出条件	使用エントリ数	
		通常フロー検出条件	重要フロー検出条件
「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定しない	指定なし	1	-
	「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定しない	1	1
	「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定	1	M※
「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定	指定なし	N※	-
	「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定しない	N※	1
	「表 3-92 複数エントリを使用するフロー検出条件」のパラメータを指定	N※	M※

(凡例)

- : 該当なし

N : 通常フロー検出条件での使用エントリ数

M : 重要フロー検出条件での使用エントリ数

注※ 各パラメータで使用するエントリ数を掛け合わせた値

(b) 帯域監視機能でのエントリ数

QoS での帯域監視機能を指定可能なフローリストの最大エントリ数は，4,000 エントリです。

なお，フロー検出条件および指定した帯域監視機能によって，1 リストで使用するエントリ数が異なります。

複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-94 複数エントリを使用するフロー検出条件

指定するフロー検出条件	使用エントリ数算出例
VLAN 番号を指定	設定した VLAN 番号数分エントリを使用します。例えば，vlan 1-2 と指定すると，使用エントリ数は 2 となります。 また，vlan と指定した場合の使用エントリ数は，インタフェース名を指定したときは 1 エントリ，物理ポートを指定したときは，指定した物理ポートが所属する VLAN 数となります。
宛先 IPv6 アドレス， 送信元 IPv6 アドレスに pd_prefix を指定	IPv6 DHCP サーバ機能によって，指定したインタフェース名で配布可能な IPv6 プレフィックス数が使用エントリ数となります。 例えば，pd_prefix を指定したインタフェース名に，コンフィグレーション dhcp6_server で，100 個のプレフィックスが割り当てられていた場合，使用エントリ数は 100 となります。

「表 3-95 複数エントリを使用するフロー検出条件」に示したフロー検出条件のパラメータを通常フロー

検出条件への指定有無と重要パケット保護機能の使用有無によって，１リストで使用する帯域監視機能での使用エントリ数が決定します。

なお，「表 3-96　1 リストで使用する帯域監視機能のエントリ数」内 N は，「表 3-95　複数エントリを使用するフロー検出条件」に該当するフロー検出条件の指定方法を二つ以上使用した場合は，各パラメータで使用するエントリ数を掛け合わせた値となり，一つの場合は，そのパラメータで使用するエントリ数となります。

表 3-95　1 リストで使用する帯域監視機能のエントリ数

項番	通常フロー検出条件	重要フロー検出条件	帯域監視設定条件	使用エントリ数
1	「表 3-95　複数エントリを使用するフロー検出条件」のパラメータを指定しない	指定なし	最大帯域制限	1
			最低帯域監視	1
			最大帯域制限＋最低帯域監視	2
2		指定あり	最大帯域制限	2
			最低帯域監視	2
			最大帯域制限＋最低帯域監視	4
3	「表 3-95　複数エントリを使用するフロー検出条件」のパラメータを指定	指定なし	最大帯域制限	N※1
			最低帯域監視	N※1
			最大帯域制限＋最低帯域監視	2 × N※1
4		指定あり	最大帯域制限	2 × N※2
			最低帯域監視	2 × N※2
			最大帯域制限＋最低帯域監視	4 × N※2

注※ 1
各パラメータで使用するエントリ数を掛け合わせた値。

注※ 2
pd_prefix は重要パケット保護機能と同時に使用できないため，ここでの N は設定した VLAN 番号数となります。例えば，vlan 1-2 と指定すると，N=2 となります。

(c) ポリシー機能のエントリ数

フィルタにおけるポリシー機能指定可能なフローリストの最大エントリ数は，1,000 エントリです。なお，フロー条件によって，1 リストで使用するエントリ数が異なります。1 リストで使用するポリシー機能のエントリ数を次の表に示します。

表 3-96　1 リストで使用するポリシー機能のエントリ数

フロー検出条件	使用エントリ数
VLAN 番号以外を指定	1
VLAN 番号を指定※	N※

注※
設定した VLAN 番号数分エントリを使用します。例えば，vlan 10-15 と指定すると，使用エントリ数は N=6 となります。

(d) NetFlow 統計のエントリ数

NetFlow 統計の最大エントリ数を次の表に示します。

NetFlow 統計のエントリは QoS とエントリを共用します。したがって，NetFlow 統計での使用エントリ数と QoS で使用しているエントリ数の合計が，最大エントリ数を超えた設定はできません。

表 3-97　SB-5400S の収容条件

BCU 搭載 メモリ量	NetFlow 統計単独使用時の最大エントリ数および NetFlow 統計・QoS 同時使用時の装置当たりの最大エントリ数 （NetFlow 統計と QoS エントリの合計）
	装置当たり
256MB	2,000
512MB	4,000
768MB	4,000
1024MB	4,000

(19) ダイナミックエントリ，スタティックエントリの最大エントリ数

ダイナミックエントリとスタティックエントリの最大エントリ数を次の表に示します。ダイナミックエントリとスタティックエントリの合計値が，最大装置エントリ数を超えないように使用してください。最大エントリ使用時は「(12) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」に示す搭載メモリ量が必要です。

表 3-98　ダイナミック・スタティック最大エントリ数

項目	最大装置 エントリ数	最大ダイナミック エントリ数	最大スタティック エントリ数
FDB	※	※	-
IPv4 ユニキャスト経路エントリ	45,000/ 装置	45,000/ 装置	2,048/ 装置
IPv4 マルチキャスト経路エントリ	8,000/ 装置	8,000/ 装置	-
IPv6 ユニキャスト経路エントリ	16,384/ 装置	16,384/ 装置	2,048/ 装置
IPv6 マルチキャスト経路エントリ	8,000/ 装置	8,000/ 装置	-
ARP	32,768/ 装置	32,768/ 装置	4,096/ 装置
NDP	8,192/ 装置	8,192/ 装置	1,024/ 装置

(凡例)　- : 該当なし

注※
「表 3-64　FDB に登録できる MAC アドレスのエントリ数」を参照してください。

(20) DHCPv6 サーバ (Prefix delegation) の収容条件

DHCPv6 サーバ (Prefix delegation) の最大配布可能 Prefix 数とインタフェース数を次の表に示します。

表 3-99　DHCPv6 サーバ収容条件

項目	最大数
最大配布可能 Prefix 数	1,024 個
インタフェース数	1,024/ 装置

（21）DHCP サーバの収容条件

DHCP サーバの収容条件を次の表に示します。

表 3-100　DHCP サーバ収容条件

項目	最大数
最大配布可能 IP アドレス数	2,000 個
最大固定 IP アドレス割り当て数	320 個
最大インタフェース数	64/ 装置
最大管理サブネット数	64/ 装置

（22）IGMP snooping/MLD snooping の収容条件

IGMP snooping 収容条件を次の表に示します。IGMP snooping で学習したマルチキャスト MAC アドレスは FDB に登録します。登録可能なマルチキャスト MAC アドレス数は IGMP snooping と IPv4 マルチキャストを同時に使用する場合に表に示すとおりになります。

表 3-101　IGMP snooping の収容条件

項目	最大数
設定 VLAN 数※ 1	128(64)
登録エントリ数※ 2	IPv4 マルチキャストを同時に使用しない：4,000(1,600) IPv4 マルチキャストを同時に使用する　：2,000

注

（ ）内の数値は，BCU の実装メモリが 256MB の場合の最大数です。

注※ 1

snooping が動作するポート数（snooping 設定 VLAN に収容されるポートの総和）は装置全体で最大 2,048(BCU 実装メモリが 256MB の場合は 1,024) です。例えば，各々 20 ポート収容している 64 個の VLAN の snooping を動作させる場合，snooping 動作ポート数は 1,280 となります。

注※ 2

各 VLAN で学習したマルチキャスト MAC アドレスの総和です。登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャスト MAC アドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャスト MAC アドレス分だけエントリを使用します。

MLD snooping 収容条件を次の表に示します。MLD snooping で学習したマルチキャスト MAC アドレスは FDB に登録します。登録可能なマルチキャスト MAC アドレス数は MLD snooping と IPv6 マルチキャストを同時に使用する場合に表に示すとおりになります。

表 3-102　MLD snooping の収容条件

項目	最大数
設定 VLAN 数※1	128(64)
登録エントリ数※2	IPv6 マルチキャストを同時に使用しない：4,000 (1,600) IPv6 マルチキャストを同時に使用する　：2,000

注
( ) 内の数値は，BCU の実装メモリが 256MB の場合の最大数です。

注※ 1
snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 2,048(BCU 実装メモリが 256MB の場合は 1,024) です。例えば，各々 20 ポート収容している 64 個の VLAN の snooping を動作させる場合，snooping 動作ポート数は 1,280 となります。

注※ 2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャスト MAC アドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャスト MAC アドレス分だけエントリを使用します。

(23) IEEE 802.1X

- BCU メモリ
  本機能は BCU メモリが 512MByte 以上必要です。もし，BCU メモリが 256MByte で動作させた場合，本機能および他機能の動作保証はしません。
- 最大認証端末数
  VLAN 単位認証を使用する場合，IEEE 802.1X を設定可能な装置当たりの総ポート数 (ポート単位認証の設定されたポート数と VLAN 単位認証の設定された VLAN の持つポート数の合計) は最大 2048 ポートです。この値は 1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば，一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合，その 10 個の VLAN で VLAN 単位認証を動作させると，総ポート数は 10 ポートになります。本装置の最大認証端末数を次の表に示します。

表 3-103　本装置の最大認証端末数

項目	最大認証端末数
装置当たり	8,192 端末
ポート単位認証当たり	256 端末
VLAN 単位認証（静的）当たり	256 端末

(24) LLDP 機能の収容条件

LLDP 機能では，隣接装置情報の最大収容数は装置当たり 384 です。

(25) OADP 機能の収容条件

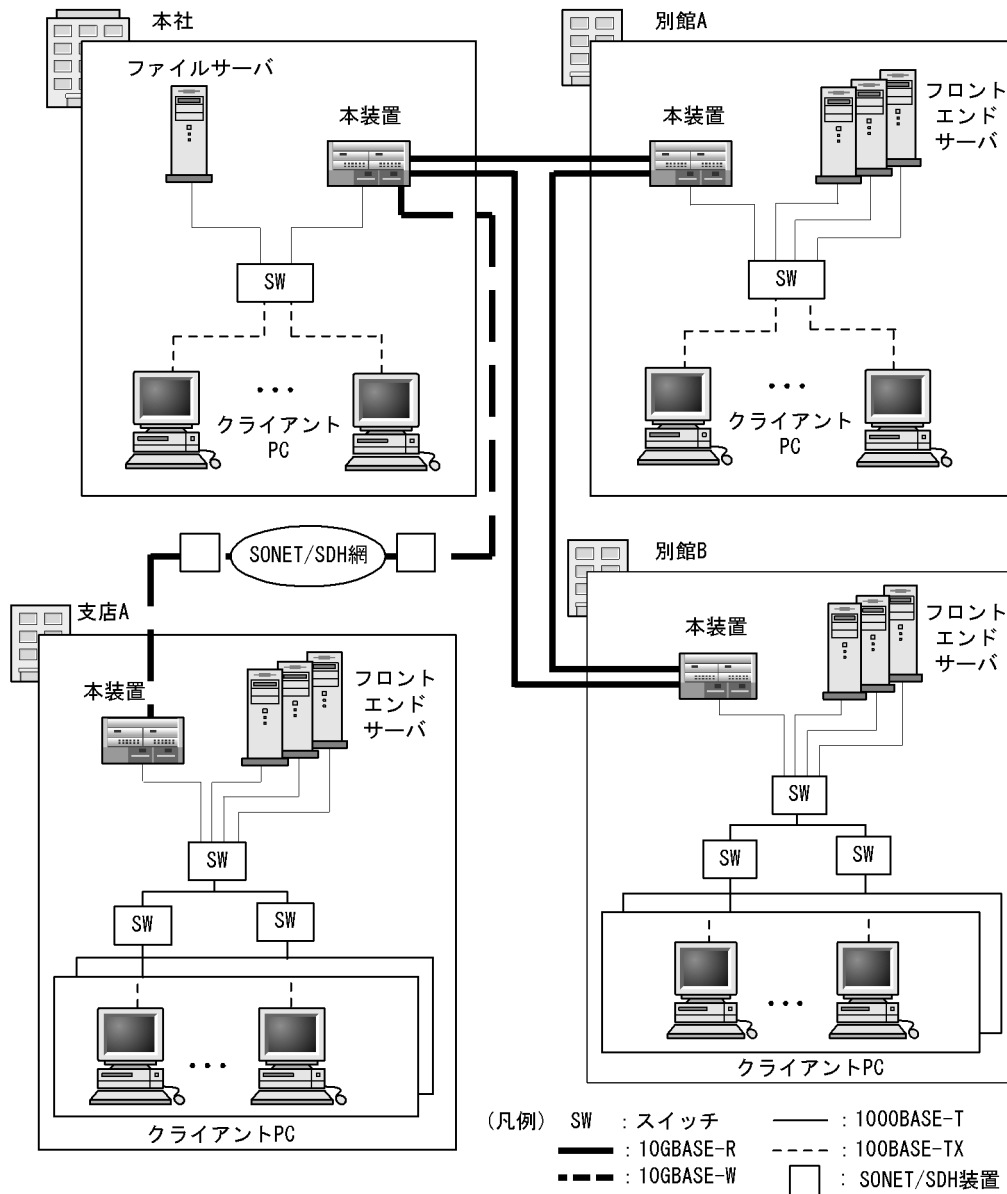
OADP 機能では，隣接装置情報の最大収容数は装置当たり 500 です。

4 イーサネット

この章では本装置のイーサネットについて説明します。

4.1 ネットワーク構成例

本装置を使用した代表的なイーサネットの構成例を次の図に示します。各ビル間，サーバ間を10GBASE-R および 10GBASE-W で接続することによって，10BASE-T/100BASE-TX/1000BASE-T および 1000BASE-X よりもサーバ間のパフォーマンスが向上します。

図 4-1 イーサネットの構成例

4.2 物理インタフェース

イーサネットには次の 3 種類があります。

- IEEE802.3 に準拠した 10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブル（UTP）を使用したインタフェース
- IEEE802.3 に準拠した 1000BASE-X の光ファイバを使用したインタフェース
- IEEE802.3ae に準拠した 10GBASE-R および 10GBASE-W の光ファイバを使用したインタフェース

4.2.1 10BASE-T ／ 100BASE-TX ／ 1000BASE-T

10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブル（UTP）を使用したインタフェースについて説明します。

（1） 接続インタフェース

（a） 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 自動認識 (オートネゴシエーション)

10BASE-T ／ 100BASE-TX ／ 1000BASE-T では自動認識機能 (オートネゴシエーション) と固定接続機能をサポートしています。

- 自動認識・・・10BASE-T，100BASE-TX，1000BASE-T（全二重）
- 固定接続・・・10BASE-T，100BASE-TX

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

（b） 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 接続仕様

本装置のコンフィグレーション指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次の表に示します。

10BASE-T および 100BASE-TX は，相手装置によってオートネゴシエーションでは接続できない場合がありますので，できるだけ相手装置のインタフェースに合わせた固定設定にしてください。

1000BASE-T は，全二重のオートネゴシエーションだけの接続となります。

表 4-1 伝送速度および，全二重および半二重モードごとの接続仕様

接続装置		本装置の設定				
設定	インタフェース	固定				オートネゴシエーション
		10BASE-T 半二重※1	10BASE-T 全二重	100BASE-TX 半二重※1	100BASE-TX 全二重	
固定	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重※2
	10BASE-T 全二重	×	10BASE-T 全二重	×	×	×
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重※2
	100BASE-TX 全二重	×	×	×	100BASE-TX 全二重	×
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	×
オートネゴシエーション	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重※2
	10BASE-T 全二重	×	×	×	×	10BASE-T 全二重
	10BASE-T 全二重および半二重	10BASE-T 半二重	×	×	×	10BASE-T 全二重
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重※2
	100BASE-TX 全二重	×	×	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	10/100BASE-TX 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	1000BASE-T 全二重
	1000BASE-T 全二重および半二重	×	×	×	×	1000BASE-T 全二重
	10/100/1000BASE-T 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	1000BASE-T 全二重※3

（凡例） ×：接続できない

注※ 1

NFMX-34 の Line 番号 32 〜 Line 番号 33 の場合，10BASE-T 半二重 /100BASE-TX 半二重は接続できません。本

装置のコンフィグレーションに 10BASE-T 半二重 /100BASE-TX 半二重を設定しないでください。

注※ 2

NFMX-34 の Line 番号 32 〜 Line 番号 33 の場合，「×：接続できない」となります。

注※ 3

本装置のインタフェースが 10BASE-T/100BASE-TX の場合 100BASE-TX 全二重となります。

(2) オートネゴシエーション

オートネゴシエーションは，伝送速度および，全二重および半二重モード認識およびフローコントロールについて，対向装置間でやりとりを行い，接続動作を決定する機能です。

本装置での接続仕様を，「表 4-1　伝送速度および，全二重および半二重モードごとの接続仕様」に示します。また本装置では，ネゴシエーション解決できなかった場合，リンク接続されるまで接続動作を繰り返し行います。

(3) フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。この機能は全二重だけサポートします。

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信でそれぞれ設定でき，有効または無効および，ネゴシエーション結果により決定したモードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば，本装置のポーズパケット送信を enable に設定した場合，相手装置のポーズパケット受信は enable と設定してください。本装置と相手装置の設定内容と実行動作モードを「表 4-2　フローコントロールの送信動作」，「表 4-3　フローコントロールの受信動作」および「表 4-4　オートネゴシエーション時のフローコントロール動作」に示します。

表 4-2　フローコントロールの送信動作

本装置のポーズパケット送信	相手装置のポーズパケット受信	フローコントロール動作
enable	enable	相手装置が送信規制を行う
disable	disable	相手装置が送信規制を行わない
desired	desired	相手装置が送信規制を行う

（凡例）

enable：有効。

disable：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-4　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-4　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 4-3　フローコントロールの受信動作

本装置のポーズパケット受信	相手装置のポーズパケット送信	フローコントロール動作
enable	enable	本装置が送信規制を行う
disable	disable	本装置が送信規制を行わない
desired	desired	本装置が送信規制を行う

（凡例）

enable：有効。

disable：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-4　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-4　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 4-4　オートネゴシエーション時のフローコントロール動作

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
enable	desired	enable	enable	enable	enable	行う	行う
			disable	enable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	enable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	enable	disable	行わない	行わない
			desired	enable	enable	行う	行う
disable		enable	enable	enable	enable	行う	行う
			disable	disable	enable	行わない	行う
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	enable	行わない	行う
			desired	enable	enable	行う	行う
desired	enable	enable	enable	enable	enable	行う	行う
			disable	disable	enable	行う	行わない
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	disable	enable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	enable	行わない	行わない
			desired	enable	enable	行う	行う
	disable	enable	enable	disable	disable	行わない	行わない
			disable	disable	disable	行わない	行わない
			desired	disable	disable	行わない	行わない
		disable	enable	enable	disable	行わない	行わない

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
			disable	disable	disable	行わない	行わない
			desired	enable	disable	行う	行わない
		desired	enable	disable	disable	行わない	行わない
			disable	disable	disable	行わない	行わない
			desired	disable	disable	行わない	行わない
	desired	enable	enable	enable	enable	行う	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う

（4） AUTO-MDI ／ MDI-X

AUTO-MDI ／ MDI-X は，MDI と MDI-X を自動的に切り替える機能です。これによって，クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。半二重および全二重固定時は MDI-X となります。MDI ／ MDI-X のピンマッピングを次の表に示します。

表 4-5 MDI ／ MDI-X のピンマッピング

RJ45	MDI			MDI-X		
Pin No.	1000BASE-T	100BASE-TX	10BASE-T	1000BASE-T	100BASE-TX	10BASE-T
1	BI_DA ＋	TD ＋	TD ＋	BI_DB ＋	RD ＋	RD ＋
2	BI_DA-	TD-	TD-	BI_DB-	RD-	RD-
3	BI_DB ＋	RD ＋	RD ＋	BI_DA ＋	TD ＋	TD ＋
4	BI_DC ＋	Unused	Unused	BI_DD ＋	Unused	Unused
5	BI_DC-	Unused	Unused	BI_DD-	Unused	Unused
6	BI_DB-	RD-	RD-	BI_DA-	TD-	TD-
7	BI_DD ＋	Unused	Unused	BI_DC ＋	Unused	Unused
8	BI_DD-	Unused	Unused	BI_DC-	Unused	Unused

注 1

10BASE-T と 100BASE-TX では，送信（TD）と受信（RD）信号は別々の信号線を使用しています。

注 2

1000BASE-T では，8 ピンすべてを送信と受信が同時双方向（bi-direction）通信するため，信号名表記が異なります。（BI_Dx：双方向データ信号）

（5） ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA ～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド IP 情報の mtu パラメータを合わせて変更することで，IP パケットのフラグメント化するサイズを大きくすることも可能となります。

本装置では，Ethernet V2 形式フレームだけサポートします。802.3 形式フレームはサポートしていません。フレームについては「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tag 付きフレームについては「4.4　VLAN-Tag」の Tag 付きフレームのフォーマットを参照してください。また，物理インタフェースは，100BASE-TX（全二重），1000BASE-T（全二重）だけサポートします。ジャンボフレームのサポート機能を次の表に示します。

表 4-6　ジャンボフレームサポート機能

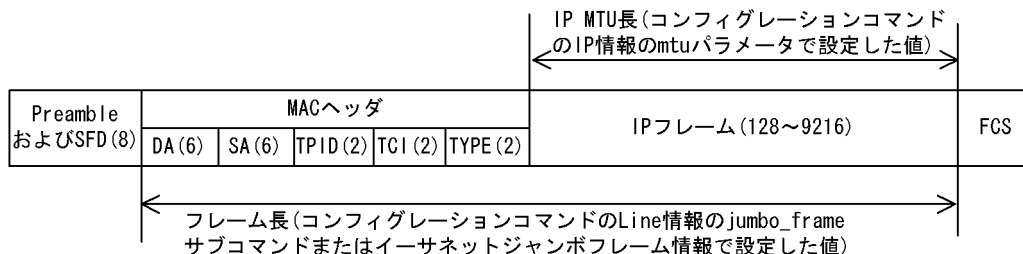
項目	フレーム形式		内容
	EthernetV2 ※1	IEEE802.3 ※1	
フレーム長 （オクテット）	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例）　○：サポート　×：未サポート
注※1　「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。

（6） フレーム長と IP MTU 長の設定時の注意事項

フレーム長および IP MTU 長の対象範囲は次に示す図のようになります。フレーム長および IP MTU 長を相手装置と合わせてください。

コンフィグレーションコマンド IP 情報の mtu パラメータを設定せずに，Line 情報の jumbo_frame サブコマンドまたはイーサネットジャンボフレーム情報を変更する場合，mtu パラメータは jumbo_frame サブコマンドに合わせ，Tag の有無に関わらず 18 オクテット減算された値となります。このため IP MTU 長を相手装置と合わせる場合は，mtu パラメータを設定してください。なお，jumbo_frame サブコマンドが mtu パラメータの最大値から 18 オクテット以上の値を設定する場合，フレーム長によらず IP MTU 長は最大値固定となります。

図 4-2　フレーム長および IP MTU 長の設定

（7） 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 接続時の注意事項

- 伝送速度，および全二重および半二重モードが相手装置と不一致の場合，接続できないので注意してく

ださい。
不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して close コマンド，free コマンドを実行してください。**【SB-7800S】**

- 100BASE-TX または 1000BASE-T を使用する場合，接続ケーブルはカテゴリ 5 以上で 8 芯 4 対のツイストペアケーブル (UTP) を使用してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。
- 1000BASE-T を使用する場合は全二重のオートネゴシエーションだけとなります。
- NFMX-34 の Line 番号 32 ～ Line 番号 33 の場合，10BASE-T 半二重 /100BASE-TX 半二重は接続できません。本装置および相手接続ポートを 10BASE-T 全二重 /100BASE-TX 全二重の固定接続，またはオートネゴシエーションに設定してください。
- NFMX-34 の Line 番号 32 ～ Line 番号 33 で，本装置がオートネゴシエーション，相手接続ポートが全二重固定接続または半二重固定接続の場合，オートネゴシエーションが失敗し，相手接続ポートがリンク接続およびリンク切断を繰り返す場合があります。相手接続ポートをオートネゴシエーションに設定するか，または本装置および相手接続ポートを全二重固定接続に設定してください。

4.2.2 1000BASE-X

1000BASE-X の光ファイバを使用したインタフェースについて説明します。

（1） 接続インタフェース

（a） 1000BASE-X

1000BASE-SX，1000BASE-LX，1000BASE-LH をサポートしています。回線速度は 1000Mbit/s 全二重固定です。

1000BASE-SX：
　短距離間を接続するために使用します。
　（マルチモード，最大 550m）

1000BASE-LX：
　中距離間を接続するために使用します。
　（シングルモード，最大 5km ／マルチモード，最大 550m）

1000BASE-LH：
　長距離間を接続するために使用します。
　（シングルモード，最大 70km）

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションになります。

- オートネゴシエーション
- 1000BASE-X 全二重固定

（b） 1000BASE-X 接続仕様

本装置のコンフィグレーション指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を「表 4-7　伝送速度および，全二重および半二重モードごとの接続仕様」に示します。なお，1000BASE-X の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

表 4-7　伝送速度および，全二重および半二重モードごとの接続仕様

接続装置側設定		本装置の設定	
設定	インタフェース	固定	オートネゴシエーション
		1000BASE 全二重	1000BASE 全二重
固定	1000BASE 半二重	×	×
	1000BASE 全二重	1000BASE 全二重	×
オートネゴシエーション	1000BASE 半二重	×	×
	1000BASE 全二重	×	1000BASE 全二重

（凡例）　×：接続できない

（2） オートネゴシエーション

オートネゴシエーションは，全二重モード選択およびフローコントロールについて，対向装置間でやりとりを行い，接続動作を決定する機能です。

本装置での接続仕様を，「表 4-7　伝送速度および，全二重および半二重モードごとの接続仕様」に示します。また本装置では，ネゴシエーション解決できなかった場合，リンク接続されるまで接続動作を繰り返し行います。

（3） フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。この機能は全二重だけサポートします。

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信でそれぞれ設定でき，有効または無効および，ネゴシエーション結果によって決定したモードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば，本装置のポーズパケット送信を enable に設定した場合，相手装置のポーズパケット受信は enable と設定してください。本装置と相手装置の設定内容と実行動作モードを「表 4-8　フローコントロールの送信動作」,「表 4-9　フローコントロールの受信動作」および「表 4-10　オートネゴシエーション時のフローコントロール動作」に示します。

表 4-8　フローコントロールの送信動作

本装置のポーズパケット送信	相手装置のポーズパケット受信	フローコントロール動作
enable	enable	相手装置が送信規制を行う
disable	disable	相手装置が送信規制を行わない
desired	desired	相手装置が送信規制を行う

（凡例）

enable：有効。ただし，シェーパ付き SFP(NE1GSHP-4S) の場合 desired と同じ動作をします。

disable：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコント

ロール動作は「表 4-10　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-10　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 4-9　フローコントロールの受信動作

本装置のポーズパケット受信	相手装置のポーズパケット送信	フローコントロール動作
enable	enable	本装置が送信規制を行う
disable	disable	本装置が送信規制を行わない
desired	desired	本装置が送信規制を行う

（凡例）

enable：有効。ただし，シェーパ付き SFP(NE1GSHP-4S) の場合 desired と同じ動作をします。

disable：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-10　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 4-10　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 4-10　オートネゴシエーション時のフローコントロール動作

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
enable	desired	enable	enable	enable	enable	行う	行う
			disable	enable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	enable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	enable	disable	行わない※	行わない
			desired	enable	enable	行う	行う
disable		enable	enable	enable	enable	行う	行う
			disable	disable	enable	行わない	行う
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	enable	行わない	行う
			desired	enable	enable	行う	行う
desired	enable	enable	enable	enable	enable	行う	行う
			disable	disable	enable	行う※	行わない
			desired	enable	enable	行う	行う

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
		disable	enable	enable	enable	行わない	行う
			disable	disable	enable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	enable	行わない※	行わない
			desired	enable	enable	行う	行う
	disable	enable	enable	disable	disable	行わない	行わない
			disable	disable	disable	行わない	行わない
			desired	disable	disable	行わない	行わない
		disable	enable	enable	disable	行わない	行わない
			disable	disable	disable	行わない	行わない
			desired	enable	disable	行う	行わない
		desired	enable	disable	disable	行わない	行わない
			disable	disable	disable	行わない	行わない
			desired	disable	disable	行わない	行わない
	desired	enable	enable	enable	enable	行う	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		disable	enable	enable	enable	行わない	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う
		desired	enable	enable	enable	行う	行う
			disable	disable	disable	行わない	行わない
			desired	enable	enable	行う	行う

注※　シェーパ付き SFP(NE1GSHP-4S) の場合は，本装置の送信規制は行いません。

(4) ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA ～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド IP 情報の mtu パラメータを合わせて変更することで，IP パケットのフラグメント化するサイズを大きくすることも可能となります。

本装置では，Ethernet V2 形式フレームだけサポートします。802.3 形式フレームはサポートしていません。フレームについては「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tag 付きフレームについては「4.4　VLAN-Tag」の Tag 付きフレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 4-11 ジャンボフレームサポート機能

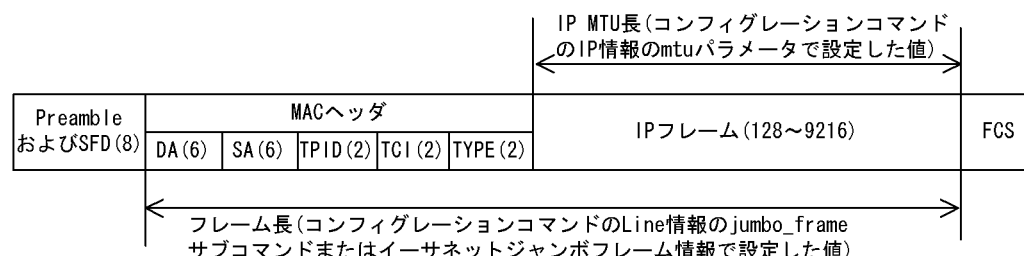
項目	フレーム形式		内容
	EthernetV2※	IEEE802.3※	
フレーム長 （オクテット）	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例） ○：サポート ×：未サポート
注※ 「4.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。

（5） フレーム長と IP MTU 長の設定時の注意事項

フレーム長および IP MTU 長の対象範囲は次に示す図のようになります。フレーム長および IP MTU 長を相手装置と合わせてください。

コンフィグレーションコマンド IP 情報の mtu パラメータを設定せずに，Line 情報の jumbo_frame サブコマンドまたはイーサネットジャンボフレーム情報を変更する場合，mtu パラメータは jumbo_frame サブコマンドに合わせ，Tag の有無に関わらず 18 オクテット減算された値となります。このため IP MTU 長を相手装置と合わせる場合は，mtu パラメータを設定してください。なお，jumbo_frame サブコマンドが mtu パラメータの最大値から 18 オクテット以上の値を設定する場合，フレーム長によらず IP MTU 長は最大値固定となります。

図 4-3 フレーム長および IP MTU 長の設定

（6） 1000BASE-X 接続時の注意事項

- 全二重のオートネゴシエーションおよび固定接続だけサポートします。
- 相手装置（スイッチングハブなど）をオートネゴシエーションまたは全二重固定に設定してください。
- マニュアル「ハードウェア取扱説明書」に示す GBIC および SFP 以外を使用した場合の動作は保証できません。
- 1000BASE-LH の光インタフェースは規格化されていないため，本装置の独自仕様となっています。

4.2.3 10BASE-T/100BASE-TX/1000BASE-T・1000BASE-X 選択型インタフェース【SB-5400S】

NFMX-34 は，1 枚の NIF で柔軟にネットワークを構築できるよう 10BASE-T/100BASE-TX/1000BASE-T インタフェース 32 回線以外に 10BASE-T/100BASE-TX/1000BASE-T または

1000BASE-X(SFP) を選択できる 1Gbit/s のワイヤレートを保証したインタフェース 2 回線を収容しています。

コンフィグレーションコマンドの Line 情報の回線種別で，10BASE-T/100BASE-TX/1000BASE-T または 1000BASE-X(SFP) を選択します。

デフォルト（Line 情報が未設定）の状態では，1000BASE-X(SFP) として動作します。

また，運用コマンド，ログメッセージおよび MIB で表示する回線情報は，コンフィグレーションで選択したコネクタ側の情報を表示します。

4.2.4 10 ギガビット・イーサネット (10GBASE-R)【SB-7800S】

10GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1) 接続インタフェース

(a) 10GBASE-R

10GBASE-SR，10GBASE-LR，10GBASE-ER をサポートしています。回線速度は 10Gbit/s 全二重固定です。

10GBASE-SR：
短距離間を接続するために使用します。（マルチモード，伝送距離 300m）

10GBASE-LR：
中距離間を接続するために使用します。（シングルモード，伝送距離 10km）

10GBASE-ER：
長距離間を接続するために使用します。（シングルモード，伝送距離 40km）

(b) 10GBASE-R 接続仕様

本装置の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

(2) フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信とでそれぞれ設定でき，有効または無効モードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば，本装置のポーズパケット送信を enable に設定した場合，相手装置のポーズパケット受信は enable と設定してください。本装置と相手装置の設定内容と実行動作を「表 4-12　フローコントロールの送信動作」および「表 4-13　フローコントロールの受信動作」に示します。

表 4-12　フローコントロールの送信動作

本装置のポーズパケット送信	相手装置のポーズパケット受信	フローコントロール動作
enable	enable	相手装置が送信規制を行う
disable	disable	相手装置が送信規制を行わない

（凡例） enable：有効 disable：無効

表 4-13 フローコントロールの受信動作

本装置のポーズパケット受信	相手装置のポーズパケット送信	フローコントロール動作
enable	enable	本装置が送信規制を行う
disable	disable	本装置が送信規制を行わない

（凡例） enable：有効 disable：無効

(3) ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA ～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド IP 情報の mtu パラメータを合わせて変更することで，IP パケットのフラグメント化するサイズを大きくすることも可能となります。

本装置では，Ethernet V2 形式フレームだけサポートします。802.3 形式フレームはサポートしていません。Tag 付きフレームで TPID が 0x8100 の場合は設定したフレーム長より 4 加算した値まで受信します。フレームについては「4.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tag 付きフレームについては「4.4 VLAN-Tag」の Tag 付フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 4-14 ジャンボフレームサポート機能

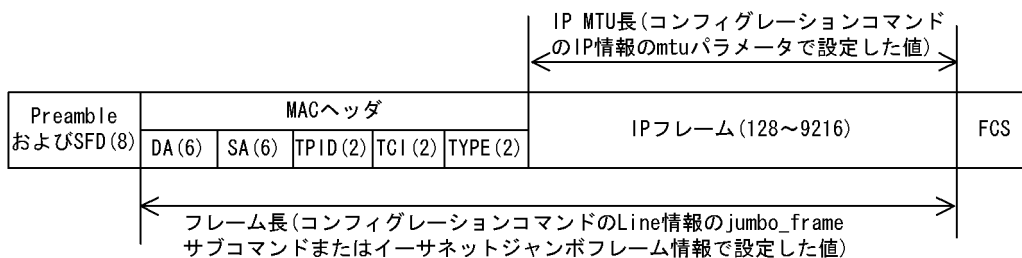
項目	フレーム形式			内容
	EthernetV2※		IEEE802.3※	
送信フレーム長（オクテット）	Tag なし	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
	Tag 付き (TPID=0x8100 以外)			
	Tag 付き (TPID=0x8100)			
受信フレーム長（オクテット）	Tag なし	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
	Tag 付き (TPID=0x8100 以外)			
	Tag 付き (TPID=0x8100)	1523 ～ 9600		
受信機能	○		×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○		×	IEEE802.3 フレームは送信しません。

（凡例） ○：サポート ×：未サポート
注※ 「4.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。

（4） フレーム長と IP MTU 長の設定時の注意事項

フレーム長および IP MTU 長の対象範囲は次に示す図のようになります。フレーム長および IP MTU 長を相手装置と合わせてください。

コンフィグレーションコマンド IP 情報の mtu パラメータを設定せずに，Line 情報の jumbo_frame サブコマンドまたはイーサネットジャンボフレーム情報を変更する場合，mtu パラメータは jumbo_frame サブコマンドに合わせ，Tag の有無に関わらず 18 オクテット減算された値となります。このため IP MTU 長を相手装置と合わせる場合は，mtu パラメータを設定してください。なお，jumbo_frame サブコマンドが mtu パラメータの最大値から 18 オクテット以上の値を設定する場合，フレーム長によらず IP MTU 長は最大値固定となります。

図 4-4　フレーム長および IP MTU 長の設定

（5） 10GBASE-R 接続時の注意事項

- 10GBASE-R の半二重およびオートネゴシエーションは IEEE802.3ae 規格上なく，全二重固定接続だけとなります。
- トランシーバが交換可能な NIF の場合，マニュアル「ハードウェア取扱説明書」に示す XFP 以外を使用した場合の動作は保証できません。

4.2.5　10 ギガビット・イーサネット WAN(10GBASE-W)【SB-7800S】

イーサネットは，従来 LAN に用途が限定されていましたが，10 ギガビットイーサネットでは，従来のイーサネットとの互換性を考慮した 10GBASE-R/10GBASE-X と，WAN で広く使用される SONET/SDH フレームを使用した 10GBASE-W が IEEE802.3ae で規格化されました。

本章では，10GBASE-W の光ファイバを使用したインタフェースについて説明します。

10GBASE-W は，WAN 用の物理層（WAN PHY）を使用することで，ペイロードのイーサネットフレームを SONET/SDH フレームでカプセリングし通信を行います。これによって，ペイロードのインタフェース速度は，9.58464Gbit/s となります。本装置では SONET/SDH 網とのシームレスな接続が可能となります。また，物理層において WAN に近い信頼性の確保も可能となります。

（1） 接続インタフェース

（a） 10GBASE-W

本装置の 10GBASE-W ファミリーでは 10GBASE-LW，10GBASE-EW をサポートしています。インタフェース速度は 10Gbit/s 全二重固定です。

10GBASE-LW：

　中距離間を接続するために使用します。例えば，中距離間の他事業所または支店間接続用として使用します。

10GBASE-EW：

長距離間を接続するために使用します。例えば，長距離間の他事業所または支店間接続用として使用します。

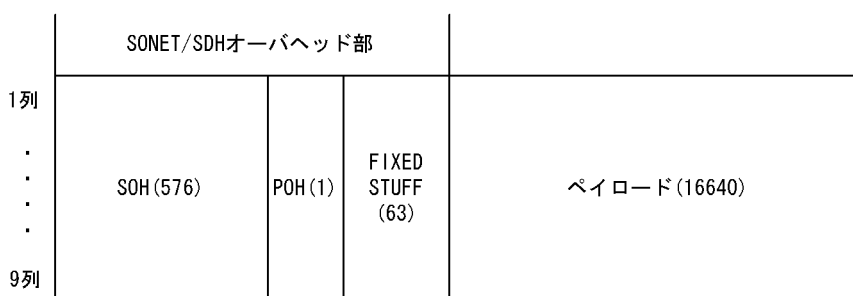
(b) 10GBASE-W 接続仕様

本装置の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

(c) フレームフォーマット

ペイロードのイーサネットフレームは，IEEE802.3ae で規定された SONET/SDH フレームでカプセリングします。フレームフォーマットを次の図に示します。なお，ペイロードのインタフェース速度は，SONET/SDH フレームでカプセリングしているため，9.58464Gbit/s となります。

図 4-5　10GBASE-W のフレームフォーマット

	SONET/SDHオーバヘッド部			
1列 ・ ・ ・ ・ 9列	SOH(576)	POH(1)	FIXED STUFF (63)	ペイロード(16640)

（凡例）（ ）内の数字はフィールド長を示します(単位:バイト)。

- SOH

  セクションオーバヘッドを示します。セクションオーバヘッドのフォーマットを次の図に示します。

図 4-6　セクションオーバヘッドのフレームフォーマット

(単位:バイト)

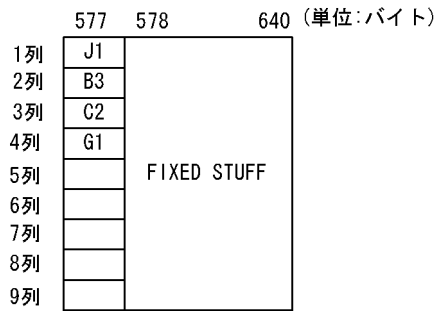
	1	2		192	193	194	195		384	385	386		576
1列	A1	A1	・・・	A1	A2	A2	A2	・・・	A2	J0	Z0	・・・	Z0
2列	B1												
3列													
4列	H1	H1	・・・	H1	H2	H2	H2	・・・	H2	H3	H3	・・・	H3
5列	B2	B2	・・・	B2	K1					K2			
6列													
7列													
8列													
9列	S1						M1						

空欄は未使用バイトを示します。

- POH

  パスオーバヘッドを示します。パスオーバヘッドのフォーマットを次の図に示します。パスオーバヘッドの各バイトの機能を「表 4-15　フレームフォーマットの詳細情報」に示します。

図 4-7　パスオーバヘッドのフレームフォーマット

	577	578　640（単位：バイト）
1列	J1	FIXED STUFF
2列	B3	
3列	C2	
4列	G1	
5列		
6列		
7列		
8列		
9列		

空欄は未使用バイトを示します。

- ペイロード
  イーサネットフレームが入ります。イーサネットフレームについては「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。

(d)　フレームフォーマットの詳細情報

SONET/SDH フレームは，IEEE802.3ae で規定された情報が設定されています。SONET/SDH 装置との接続の際は，フレームフォーマットの詳細情報を確認の上設定してください。

表 4-15　フレームフォーマットの詳細情報

項目		バイト名称	IEEE802.3ae 規格	本装置	
				仕様	デフォルト値
パスシグナルラベル	送信値	C2	1A	00 ～ FF	1A
	P-PLM 障害検出		検出する	検出する	-
パスステータス	P-ERDI 転送（3bit モード）	G1	3bit モード	1 or 3bit モード	3bit モード
	P-RDI 転送（1bit モード）				
セクショントレース	送信メッセージトレースモード	J0，Z0	16 オクテット	1 オクテット or 16オクテット or C1 バイト	16 オクテット
	1 オクテット（16 進数）	J0	規定なし	00 ～ FF	J0：890000000000000000000000 0000000 Z0：CC
		Z0		CC	
	16 オクテット（16 進数）	J0	890000000000000000000000 00000000	890000000000000000000000 0000000	
		Z0	CC	CC	
	C1 バイト（16 進数）	J0	規定なし	01	
		Z0		02,03・・・C0 ※	
	受信メッセージトレースモード	J0	16 オクテット	1 オクテット or 16オクテット or C1 バイト	16 オクテット
パストレース	送信メッセージトレースモード	J1	16 オクテット	1 オクテット or 16 オクテット	16 オクテット

項目		バイト名称	IEEE802.3ae 規格	本装置	
				仕様	デフォルト値
	1 オクテット (16 進数)		規定なし	00 ～ FF	890000000000 000000000000 00000000
	16 オクテット (16 進数)		890000000000 000000000000 00000000	890000000000 000000000000 00000000	
	受信メッセージトレースモード		16 オクテット	1 オクテット or 16 オクテット	16 オクテット
H1 ポインタ内の SS ビット (2 進数)		H1	10	00 or 10	10

（凡例） - : 該当なし

注※　Z0 バイトにそれぞれ 02H から 01H ずつ加算し，C0H までの値が入ります。

(2) フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信とでそれぞれ設定でき，有効または無効モードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば，本装置のポーズパケット送信が enable に設定した場合，相手装置のポーズパケット受信は enable と設定してください。

本装置と相手装置の設定内容と実行動作を「表 4-16　フローコントロールの送信動作」および「表 4-17　フローコントロールの受信動作」の表にそれぞれ示します。

表 4-16　フローコントロールの送信動作

本装置のポーズパケット送信	相手装置のポーズパケット受信	フローコントロール動作
enable	enable	相手装置が送信規制を行う
disable	disable	相手装置が送信規制を行わない

（凡例） enable : 有効　disable : 無効

表 4-17　フローコントロールの受信動作

本装置のポーズパケット受信	相手装置のポーズパケット送信	フローコントロール動作
enable	enable	本装置が送信規制を行う
disable	disable	本装置が送信規制を行わない

（凡例） enable : 有効　disable : 無効

(3) ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA ～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド IP 情報の mtu パラメータを合わせて変更することで，IP パケットのフラグメント化するサイズを大きくすることも可能となります。

本装置では，Ethernet V2 形式フレームだけサポートします。802.3 形式フレームはサポートしていません。Tag 付フレームで TPID が 0x8100 の場合は設定したフレーム長より 4 加算した値まで受信します。フレームについては「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tag 付きフレームについては「4.4　VLAN-Tag」の Tag 付フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 4-18　ジャンボフレームサポート機能

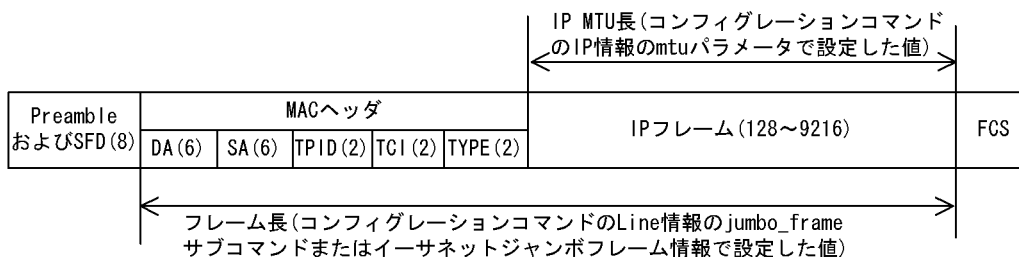
項目	フレーム形式			内容
	EthernetV2※		IEEE802.3※	
送信フレーム長（オクテット）	Tag なし	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
	Tag 付き (TPID=0x8100 以外)			
	Tag 付き (TPID=0x8100)			
受信フレーム長（オクテット）	Tag なし	1519 ～ 9596	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
	Tag 付き (TPID=0x8100 以外)			
	Tag 付き (TPID=0x8100)	1523 ～ 9600		
受信機能	○		×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○		×	IEEE802.3 フレームは送信しません。

（凡例）　○：サポート　×：未サポート
注※ 「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。

(4) フレーム長と IP MTU 長の設定時の注意事項

フレーム長および IP MTU 長の対象範囲は次の図のようになります。フレーム長および IP MTU 長を相手装置と合わせてください。

コンフィグレーションコマンド IP 情報の mtu パラメータを設定せずに，Line 情報の jumbo_frame サブコマンドまたはイーサネットジャンボフレーム情報を変更する場合，mtu パラメータは jumbo_frame サブコマンドに合わせ，Tag の有無に関わらず 18 オクテット減算された値となります。このため IP MTU 長を相手装置と合わせる場合は，mtu パラメータを設定してください。

図 4-8　フレーム長および IP MTU 長の設定

(5) クロック

本装置では，独立同期および従属同期をサポートしています。

独立同期は WDM(Wavelength Division Multiplexing) 装置および，ルータまたはスイッチと接続する場合に指定します。

従属同期は網同期で接続する場合に指定します。なお，従属同期での接続は以下の入力周波数精度の装置としてください。

- 9.95328Gbit/s ± 20ppm 以下 (Sonet Minimum Clock)

本装置のデフォルト値は独立同期です。IEEE802.3ae に準拠しています。

(6) 10GBASE-W 接続時の注意事項

- 10GBASE-W の半二重およびオートネゴシエーションは IEEE802.3ae 規格上なく，全二重固定接続だけとなります。
- ループコネクタを接続する場合はクロックを独立同期にしてください。なお，回線テストを実行する場合は，独立同期に変更しなくても実行できます。

4.2.6 RM イーサネット（SB-5400S ではリモートマネージメントポート）（10BASE-T/100BASE-TX）

RM イーサネット（SB-5400S ではリモートマネージメントポート）（10BASE-T/100BASE-TX）のツイストペアケーブル（UTP）を使用したインタフェースについて説明します。

(1) 接続インタフェース

(a) RM イーサネット（SB-5400S ではリモートマネージメントポート）機能仕様

RM イーサネットは主にリモート運用端末を接続するための RM イーサネットポートを提供します。RM イーサネット（SB-5400S ではリモートマネージメントポート）の機能仕様を次の表に示します。

表 4-19　RM イーサネット（SB-5400S ではリモートマネージメントポート）の機能仕様

機能概要	仕様
インタフェース種別	10BASE-T および 100BASE-TX
オートネゴシエーション	サポート
フローコントロール	未サポート
ジャンボフレーム	未サポート

機能概要	仕様
MAC および LLC 副層制御フレーム	Ethernet V2 形式だけ (802.3 形式，その他は未サポート)
対象プロトコル	IP
パケット中継処理	未サポート
フィルタリング	未サポート
QoS	未サポート
SNMP	dot3 グループ
Tag-VLAN 連携	未サポート
マルチキャスト	未サポート
マルチホーム	未サポート
AUTO-MDI/MDI-X	未サポート

(b) 10BASE-T ／ 100BASE-TX 自動認識 (オートネゴシエーション)

RM イーサネットでは，次の自動認識機能 (オートネゴシエーション) および固定接続機能をサポートしています。

- 自動認識・・・10BASE-T，100BASE-TX
- 固定接続・・・10BASE-T，100BASE-TX

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

(c) RM イーサネット（SB-5400S ではリモートマネージメントポート）の接続仕様

本装置のコンフィグレーション指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次の表に示します。

相手装置によってはオートネゴシエーションでは接続できない場合があるので，なるべく相手装置のインタフェースに合わせた固定設定にしてください。

表 4-20　伝送速度および，全二重および半二重モードごとの接続仕様

接続装置		本装置の設定				
設定	インタフェース	固定				オートネゴシエーション
		10BASE-T 半二重	10BASE-T 全二重	100BASE-TX 半二重	100BASE-TX 全二重	
固定	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	10BASE-T 全二重	×	×	×
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	100BASE-TX 全二重	×
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	×
オートネゴシエーション	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	×	×	×	10BASE-T 全二重
	10BASE-T 全二重および半二重	10BASE-T 半二重	×	×	×	10BASE-T 全二重
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	10/100BASE-TX 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	×
	1000BASE-T 全二重および半二重	×	×	×	×	×
	10/100/1000BASE-T 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重

（凡例）×：接続できない

(2) オートネゴシエーション

オートネゴシエーションは，伝送速度および全二重または半二重モード認識について対向装置間でやり取

りを行い，接続動作を決定する機能です。

本装置での接続仕様を「表 4-20　伝送速度および，全二重および半二重モードごとの接続仕様」に示します。また，本装置ではネゴシエーション解決できなかった場合，リンク接続されるまで接続動作を繰り返し行います。

(3) RM イーサネット（SB-5400S ではリモートマネージメントポート）接続時の注意事項

- 伝送速度または全二重および半二重モードが相手装置と不一致の場合，接続できないのでご注意ください。
- RM イーサネットポート（SB-5400S ではリモートマネージメントポート）を 100BASE-TX で使用する場合，接続ケーブルはカテゴリ 5 以上で 8 芯 4 対のツイストペアケーブル (UTP) を使用してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。
- RM イーサネット（SB-5400S ではリモートマネージメントポート）の接続に使用するツイストペアケーブルは AUTO MDI/MDI-X 未サポートのため，次に示すとおりとしてください。
  - 本装置と PC を直結する場合は，クロスケーブルを使用してください。
  - 本装置と PC を直結しない場合（スイッチやハブを経由する場合）は，ストレートケーブルを使用してください。

4.2.7 メンテナンスポート（10BASE-T/100BASE-TX）【SB-5400S】

メンテナンスポートは IPv4 による通信が可能な PC などの運用端末から，本装置に対して telnet によるログイン，および ftp によるファイル転送を行うための保守用のイーサネットポートです。このポートには固定的に IPv4 アドレスを割り付けていて，また接続装置の IP アドレスによるアクセス制限を行いませんのでコンフィグレーションを設定することなく本装置へログインすることができます。このポートを使用することによって，RS-232C 接続によるコンソール端末を接続するのと比べ，より高速な端末操作およびファイル転送を行うことができます。

表 4-21　メンテナンスポートの機能仕様

機能概要	仕様
インタフェース種別	10BASE-T および 100BASE-TX
回線種別	オートネゴシエーション
MAC/LLC 副層制御フレーム	Ethernet V2 形式
対象プロトコル	IPv4
中継処理	このポートを介した中継処理はおこないません
IP アドレスの初期設定値	BCU0 側のメンテナンスポート 192.168.0.1/24 BCU1 側のメンテナンスポート 192.168.0.2/24 (コンフィグレーションで初期値を変更することができます)

このポートにリモート運用端末を直接接続する場合には，クロスケーブルで接続してください。また，ハブやスイッチを介して接続する場合にはストレートケーブルを使用して接続してください。

4.3 MAC および LLC 副層制御

フレームフォーマットを次の図に示します。RM イーサネット（SB-5400S ではリモートマネージメントポート）では Ethernet V2 形式フレームだけをサポートしています。

図 4-9 フレームフォーマット

Preamble およびSFD(8)	MACヘッダ			DATAおよびPAD(46～9582(注1))	FCS
	DA(6)	SA(6)	TYPE/LENGTH(2)		

Ethernet V2形式フレーム時

TYPE= 0x05DD～	DATA	(PAD)

802.3形式フレーム時

LENGTH= 0x0000～ 0x05DC	LLCヘッダ			SNAPヘッダ (注2)		DATA	(PAD)
	DSAP (1)	SSAP (1)	CONTROL (1～2)	OUI (3)	PID (2)		

( )内の数字はフィールド長を示す。(単位：オクテット)

注1 DATAおよびPADの最大長はEthernetV2形式フレーム時だけ9582。
802.3形式フレームおよびその他の形式のフレームは1500。
注2 DSAPとSSAPが"AA", CONTROLが"03"のとき,
0x0000000800 (IP)
0x0000000806 (ARP)

(1) MAC 副層フレームフォーマット

(a) Preamble および SFD

64 ビット長の 2 進数で「1010...1011(最初の 62 ビットは 10 繰返し，最後の 2 ビットは 11)」のデータです。送信時にフレームの先頭に付加します。この 64 ビットパターンのないフレームは受信できません。

(b) DA および SA

48 ビット形式をサポートします。16 ビット形式およびローカルアドレスはサポートしていません。

(c) TYPE ／ LENGTH

TYPE ／ LENGTH フィールドの扱いを次の表に示します。

表 4-22 TYPE ／ LENGTH フィールドの扱い

TYPE ／ LENGTH 値	本装置での扱い
0x0000 ～ 0x05DC	IEEE802.3 CSMA/CD のフレーム長
0x05DD ～	Ethernet V2.0 のフレームタイプ

(d) FCS

32 ビットの CRC 演算を使用します。

(2) LLC 副層フレームフォーマット

IEEE802.2 の LLC タイプ 1 をサポートしています。Ethernet V2 では LLC 副層はありません。

（a） DSAP

LLC 情報部の宛先のサービスアクセス点を示します。

（b） SSAP

LLC 情報部を発信した特定のサービスアクセス点を示します。

（c） CONTROL

情報転送形式，監視形式，非番号制御形式の三つの形式を示します。

（d） OUI

SNAP 情報部を発信した組織コードフィールドを示します。

（e） PID

SNAP 情報部を発信したイーサネット・タイプ・フィールドを示します。

（3） LLC の扱い

IEEE802.2 の LLC タイプ 1 をサポートしています。また，次に示す条件に合致したフレームだけをルーティングの対象にします。次に示す条件以外のフレームは，廃棄します。

（a） DSAP，SSAP フィールド

SNAP を示す ('AA'16 進数) 値で，SSAP ＝ DSAP であることが必要です。

（b） CONTROL フィールド

CONTROL フィールドの値と送受信サポート内容を「表 4-23　CONTROL フィールドの値と送受信サポート内容」に示します。また，「表 4-23　CONTROL フィールドの値と送受信サポート内容」に示す TEST フレームおよび XID フレームについては「表 4-24　XID および TEST レスポンス」に示す形で応答を返します。

表 4-23　CONTROL フィールドの値と送受信サポート内容

種別	コード (16 進数)	コマンド	レスポンス	備考
UI	03	送信・受信 サポート	-	-
TEST	F3 または E3	受信サポート	送信サポート	IEEE802.2 の仕様に従って，TEST レスポンスを返送します。
XID	BF または AF	受信サポート	送信サポート	IEEE802.2 の仕様に従って，XID レスポンスを返送します。ただし，XID レスポンスの情報部は 129.1.0(IEEE802.2 の規定による ClassI を示す値) とします。

（凡例）- : 該当しない

表 4-24　XID および TEST レスポンス

MAC ヘッダの DA	フレーム種別	DSAP	応答
ブロードキャストまたはマルチキャスト	XID および TEST	AA(SNAP) 42(BPDU) 00(null) FF(global)	返す
		上記以外	返さない
個別アドレスで自局アドレス	XID および TEST	AA(SNAP) 42(BPDU) 00(null) FF(global)	返す
		上記以外	返さない
個別アドレスで他局アドレス	XID および TEST	すべてのアドレス	返さない

(4)　受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

- フレーム長がオクテットの整数倍でない
- 受信フレーム長 (DA ～ FCS) が 64 オクテット未満，または 1523 オクテット以上
  ただし，ジャンボフレーム選択時は，指定したフレームサイズを超えた場合
- FCS エラー
- 接続インタフェースが半二重の場合は，受信中に衝突が発生したフレーム

(5)　パッドの扱い

送信フレーム長が 64 オクテット未満の場合，MAC 副層で FCS の直前にパッドを付加します。パッドの値は不定です。

4.4　VLAN-Tag

（1）概要

IEEE 802.1Q 規定による VLAN-Tag（イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法）を使用して，一つのポートに複数の VLAN を構築できます。

VLAN-Tag は，VLAN に属するポートとして Tagged ポートを指定するか，または Tag-VLAN 連携機能を適用することによって使用します。VLAN-Tag を使用するポートはその対向装置も VLAN-Tag を認識できる必要があります。

（2）プロトコル仕様

VLAN-Tag はイーサネットフレームに Tag と呼ばれる識別子を埋め込むことで，VLAN 情報（=VLAN ID）を離れたセグメントへと伝えることができます。

VLAN-Tag 付きフレームのフォーマットを次の図に示します。VLAN-Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 4-10　VLAN-Tag 付きフレームのフォーマット

●Ethernet IIフレーム

通常のフレーム

MAC-DA（6バイト）	MAC-SA（6バイト）	Ether Type（2バイト）	IP Data（46～1500バイト）

タグフレーム

●802.3LLC/SNAPフレーム

通常のフレーム

MAC-DA（6バイト）	MAC-SA（6バイト）	Length（2バイト）	LLC（3バイト）	SNAP（5バイト）	IP Data（38～1492バイト）

タグフレーム

MAC-DA（6バイト）	MAC-SA（6バイト）	Tag（4バイト）	Length（2バイト）	LLC（3バイト）	SNAP（5バイト）	IP Data（38～1492バイト）

VLAN-Tag のフィールドの説明を次の表に示します。

表 4-25　VLAN-Tag のフィールド

フィールド	説明	本装置の条件
TPID （Tag Protocol ID）	IEEE802.1Q VLAN-Tag が続くことを示す Ether Type 値。	次に示す値をコンフィグレーションで選択できます。 • 0x8100(回線ごとのデフォルト値) • 0x9100(回線ごとに指定できます) • 任意値 (装置単位に指定できます。ただし，0x9100 指定の回線がある場合は指定できません)
User Priority	IEEE802.1D のプライオリティ。	コンフィグレーションで 8 段階のプライオリティレベルを選択できます。
CF （Canonical Format）	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかを示します。	本装置では標準 (0) だけをサポートします。
VLAN ID	所属している VLAN の番号を示します。※	ユーザが使用できる VLAN ID は 1 ～ 4,095 で，ポート当たりの最大数は 4,095 個です。

注※　Tag 変換機能を使用している場合，Tag 変換機能で設定した Translated ID を使用します。詳細は「7.5.5　Tag 変換機能」を参照してください。

4.5 本装置の MAC アドレス

(1) 装置 MAC アドレス

本装置は，装置を識別する MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは，レイヤ 3 インタフェースの MAC アドレスやスパニングツリーなどのプロトコルの装置識別子として使用します。

装置 MAC アドレスは，コンフィグレーションコマンド local-mac-address によって指定できます。コンフィグレーションコマンドで指定しない場合は，装置の持っている MAC アドレスが装置 MAC アドレスになります。そのとき使用される MAC アドレスは装置のモデルによって異なります。装置モデルごとの装置 MAC アドレスを次の表に示します。

表 4-26　コンフィグレーションコマンド local-mac-address を指定しないときの装置 MAC アドレス

装置のモデル	装置 MAC アドレス
SB-7800S	運用系 BCU の RM イーサネットの MAC アドレス
SB-5400S	シャーシの MAC アドレス

(2) 装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 4-27　装置 MAC アドレスを使用する機能

機能	用途
VLAN	レイヤ 3 インタフェースの MAC アドレス
ルータポート（リンクアグリゲーション）	レイヤ 3 インタフェースの MAC アドレス
リンクアグリゲーションの LACP	装置識別子
スパニングツリー	装置識別子
GSRP	装置識別子
LLDP	装置識別子
OADP	装置識別子
IEEE802.3ah/UDLD	装置識別子

(3) 装置 MAC アドレス使用時の注意事項

(a) コンフィグレーションコマンド local-mac-address 変更時の注意事項

装置 MAC アドレスはコンフィグレーションコマンド local-mac-address の設定，変更および削除によって値を変更できます。装置 MAC アドレスの変更の際，そのアドレスを使用する機能では，次の点に注意してください。

- レイヤ 3 インタフェースの MAC アドレスが変わるため，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと本装置の MAC アドレスが不一致となり，一時的に通信できなくなる場合があります。
- リンクアグリゲーションの LACP，スパニングツリー，GSRP の装置識別子が変わるため，プロトコルが初期状態から再開始します。そのため，一時的に通信できなくなる場合があります。
- LLDP，OADP の装置識別子が変わるため，隣接装置で変更前の MAC アドレスの情報がタイムアウト

などで削除されるまで一時的に 2 台の装置を検出している状態になる場合があります。

- IEEE802.3ah/UDLD の装置識別子が変わるため，隣接装置側で異なる装置からの情報を受信することにより，統計情報の Info TLV の Unstable が加算される場合があります。

(b) 二重化系切替時の注意事項【SB-7800S】

コンフィグレーションコマンド local-mac-address を設定していない場合，運用系 BCU の RM イーサネットの MAC アドレスを使用します。そのため，二重化系切替によって装置 MAC アドレスが，系切替後の運用系 BCU の RM イーサネットの MAC アドレスに変更になります。

4.6 リンクアグリゲーション

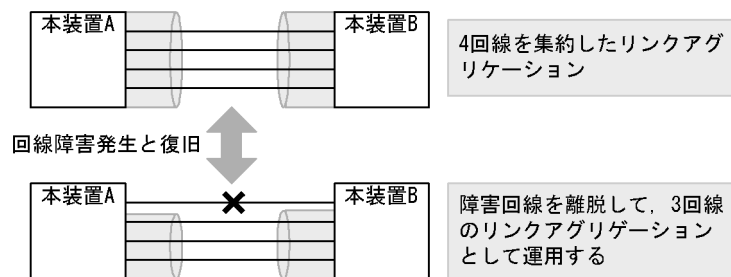
4.6.1 リンクアグリゲーション概説

(1) 概要

リンクアグリゲーションは，隣接装置との間を複数のイーサネット回線で接続し，それらを束ねて一つの仮想リンクとして扱う機能です。この仮想リンクを**リンクアグリゲーショングループ**と呼びます。リンクアグリゲーションによって接続装置間の帯域の拡大や回線冗長性を確保できます。

(2) リンクアグリゲーション構成

リンクアグリゲーションの構成例を次の図に示します。この例では 4 本の回線を集約しています。集約している回線の内の 1 本が障害となった場合には，リンクアグリゲーショングループから離脱し，残りの回線でリンクアグリゲーショングループとして通信を継続します。なお，本装置は NIF をまたがってリンクアグリゲーショングループに属する回線を設定できるので，NIF 障害によってリンクアグリゲーショングループ内の全回線が障害になることを回避できます。

図 4-11　リンクアグリゲーションの構成例

4.6.2 リンクアグリゲーション仕様

(1) リンクアグリゲーションの種類

リンクアグリゲーションのモードとして，LACP リンクアグリゲーションおよびスタティックリンクアグリゲーションをサポートします。

- LACP リンクアグリゲーション
  IEEE802.3ad 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合にリンクアグリゲーショングループとしての運用を開始します。LACP の利用によって，隣接装置との整合性確認や，リンクの正常性確認・障害検知の確度を向上できます。
- スタティックリンクアグリゲーション
  コンフィグレーションによるスタティックなリンクアグリゲーションです。LACP は動作させず，リンクアグリゲーショングループとして定義した回線がリンクアップした時点で運用を開始します。

(2) 収容条件

リンクアグリケーションの収容条件を次の表に示します。

表 4-28 リンクアグリゲーションの収容条件

項目	サポート仕様	備考
装置当たりのリンクアグリゲーショングループ数	128	LACP リンクアグリゲーションとスタティックリンクアグリゲーションの合計値
1 グループ当たりの最大ポート数	16	-
回線種別	イーサネット	-
回線速度	デフォルト時： 同一速度だけ 異速度混在モード時： 異なる速度を同時に使用します。	デフォルト時： 遅い回線は離脱します。 異速度混在モード時： 回線速度による離脱はありません。
Duplex モード	• LACP リンクアグリゲーション 全二重だけ • スタティックリンクアグリゲーション 全二重 / 半二重ともに可能。 グループ内の不一致を許容します。	-

（凡例） - : 該当しない

(3) リンクアグリゲーショングループの MAC アドレス

リンクアグリゲーション上でレイヤ 2 およびレイヤ 3 以上の上位プロトコルを運用する際に，リンクアグリゲーショングループの MAC アドレスを使用します。本装置がリンクアグリゲーショングループに割り当てる MAC アドレスを次の表に示します。

表 4-29 リンクアグリゲーショングループの MAC アドレス

ポートの種類	MAC アドレス	備考
レイヤ 2 スイッチ対象のポート※1	グループに所属するポートの内，どれかの MAC アドレス	所属するポートの追加，削除などによって，MAC アドレスが変わることがあります。
レイヤ 2 スイッチ対象外のポート※2	本装置の MAC アドレス	装置の MAC アドレスの変更によって，本 MAC アドレスが変わります。

注※ 1

レイヤ 2 スイッチ対象のポートとは，VLAN に所属するポートです。

注※ 2

レイヤ 2 スイッチ対象外のポートとは，次に示すポートです。

・回線およびリンクアグリゲーションに直に IP アドレスを設定したポート

・Tag-VLAN 連携機能を設定したポート

(4) 離脱ポート数制限機能

離脱ポート数制限機能は，回線障害が発生した回線を離脱して残りの回線で運用を継続する機能を抑止します。リンクアグリゲーションのどれかの回線に障害が発生するとグループ全体を障害とみなし，該当リンクアグリゲーショングループの運用を停止します。グループ内の全回線が復旧するとグループの運用を再開します。

GSRP などの冗長化機能と合わせて運用することで，リンクアグリゲーショングループ内の 1 回線の障害発生によって，グループ単位で切り替えることができます。

なお，この機能は LACP リンクアグリゲーションだけで動作できます。

(5) スタンバイリンク機能

リンクアグリゲーショングループ内にあらかじめ待機用の回線を用意しておき，運用中の回線が障害となったときに待機用の回線と切り替えることによってグループとして運用する回線数を維持する機能です。この機能によって，障害時に帯域の減少を防ぐことができます。なお，この機能はスタティックリンクアグリゲーションだけで動作できます。

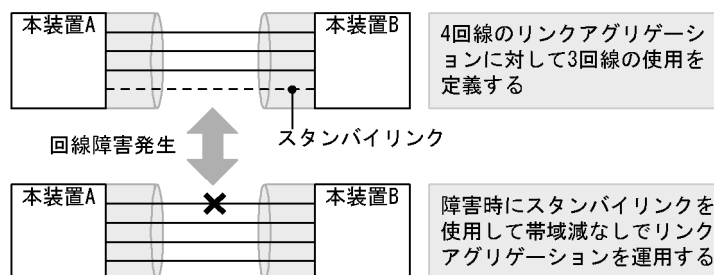
コンフィグレーションでリンクアグリゲーショングループとして運用する最大回線数を設定します。グループに属する回線数が指定された運用をする最大回線数を超えた分の回線が待機用回線となります。

待機用回線は，コンフィグレーションコマンドで設定するポート優先度，ポートの NIF 番号，または Line 番号から選択されます。待機用回線は，次に示す選択優先度の高い順に決定します。

表 4-30　待機用回線の選択方法

選択優先度	パラメータ	備考
高 ↑ ↓ 低	ポート優先度	コンフィグレーションコマンド port-priority で優先度の低いポートから選択
	NIF 番号	ポートの NIF 番号の大きい順に選択
	Line 番号	ポートの Line 番号の大きい順に選択

スタンバイリンク機能の例を次の図に示します。この例では，グループに属する回線数を 4 回線，運用する最大回線数を 3 回線としています。

図 4-12　スタンバイリンク機能の構成例

スタンバイリンク機能には，次に示す二つのモードがあります。

- リンクダウンモード
  スタンバイリンクをリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用回線にすることができます。
- 非リンクダウンモード
  スタンバイリンクをリンクダウン状態にしないで，送信だけを停止します。リンクアップ状態のため，待機中の回線でも回線障害を監視できます。また，待機中の回線は送信だけを停止して，受信は行います。スタンバイリンク機能をサポートしていない対向装置は，リンクダウンが伝わらないためスタンバイリンク上で送信を継続しますが，そのような対向装置とも接続はできます。

リンクダウンモードを使用している場合，運用中の回線が一つのとき，その回線で障害が発生すると，待機用の回線に切り替わる際にリンクアグリゲーショングループがいったんダウンします。リンクアグリゲーショングループがいったんダウンすると，FDB をクリアし，上位プロトコルでは状態変更をします。

非リンクダウンモードの場合，ダウンせずに待機用回線を使用します。

運用中の回線が一つの状態とは，次に示すどちらかの状態です。

- コンフィグレーションコマンド max-active-port で 1 を設定している状態。
- 異速度混在モードを未設定で，最高速の回線が一つだけ，そのほかの回線が一つ以上ある状態。

(6) 異速度混在モード

リンクアグリゲーションで異なる速度の回線を同時に集約して運用するモードです。この機能によって，リンクアグリゲーションで利用する回線速度を変更（ネットワーク構成の変更）する際に，リンクアグリゲーションをダウンさせないで構成を変更できます。

以下に，異速度混在モードを利用したリンクアグリゲーションの速度移行について，移行手順の具体例を示します。

1. 従来状態で運用（1Gbit/s の回線 2 ポートとします）
2. 異速度混在モードを設定
3. 当該リンクアグリゲーションに 10Gbit/s の回線 2 ポートを追加
   （コンフィグレーションコマンド link-aggregation の aggregated-port サブコマンドによる追加）
   異速度混在モード未設定時は，この手順でリンクアグリゲーションがいったんダウンします。
4. 3 で追加した 10Gbit/s の回線 2 ポートをリンクアップ
5. 従来の 1Gbit/s の回線 2 ポートをリンクダウン
6. 従来の 1Gbit/s の回線 2 ポートのコンフィグレーションコマンド link-aggregation の aggregated-port サブコマンドの指定を削除
7. 10Gbit/s の回線 2 ポートに移行完了

4.6.3 フレーム送信時のポート振り分け

リンクアグリゲーションへフレームを送信するとき，送信するフレームごとにポートを選択しトラフィックを各ポートへ分散させることで複数のポートを効率的に利用します。ポートの振り分けは，フレーム内情報による振り分け方法と VLAN ごとの振り分け方法の 2 種類があり，コンフィグレーションによってリンクアグリゲーショングループごとに指定できます。

(1) フレーム内情報によるポート振り分け

リンクアグリゲーションへフレームを送信するとき，フレーム内の情報を基にポートを選択して送信します。フレーム内の情報の参照方法はレイヤ 2 中継時と IP レイヤ中継時では異なり，レイヤ 2 中継時の参照情報を「表 4-31　レイヤ 2 中継時の参照情報」に，IP レイヤ中継時の参照情報を「表 4-32　IP レイヤ中継時の参照情報」に示します。

表 4-31　レイヤ 2 中継時の参照情報

動作分類	情報元	TCP/UDP/SCTP のフレーム	IP のフレーム (TCP/UDP/SCTP 以外)	MPLS Label Stack の付いたフレーム	その他のフレーム
中継	受信フレーム	• 宛先 MAC アドレス • 送信元 MAC アドレス • 宛先 IP アドレス • 送信元 IP アドレス • 宛先ポート番号 • 送信先ポート番号	• 宛先 MAC アドレス • 送信元 MAC アドレス • 宛先 IP アドレス • 送信元 IP アドレス	• 宛先 MAC アドレス • 送信元 MAC アドレス • MPLS Label Stack のボトムラベル	• 宛先 MAC アドレス • 送信元 MAC アドレス
自発送信	送信フレーム	-	-	-	• 宛先 MAC アドレス • 送信元 MAC アドレス

（凡例） - : 該当しない

表 4-32 IP レイヤ中継時の参照情報

動作分類	情報元	TCP/UDP/SCTP のフレーム	IP のフレーム (TCP/UDP/SCTP 以外)	MPLS Label Stack の付いたフレーム	その他のフレーム
中継	受信フレーム	• 宛先 IP アドレス • 送信元 IP アドレス • 宛先ポート番号 • 送信先ポート番号	• 宛先 IP アドレス • 送信元 IP アドレス	-	-
自発送信	送信フレーム	• 宛先 IP アドレス • 送信元 IP アドレス • 宛先ポート番号 • 送信先ポート番号	• 宛先 IP アドレス • 送信元 IP アドレス	-	-

（凡例） - : 該当しない

(2) VLAN ごとのポート振り分け

(a) 概要

リンクアグリゲーションへフレームを送信するとき，フレームを受信した VLAN ごとに送信先ポートを選択し送信します。振り分けに使用する情報は VLAN ごとに割り当てられている本装置の内部的な識別子を使用します。Tag 変換機能を使用していて異なる VLAN Tag が付与されたフレームであっても，同じ VLAN は同じポートに振り分けます。

この振り分けモードでの動作を次の表に示します。IP レイヤ中継の場合，フレームを受信した VLAN と送信する VLAN は異なることに注意してください。レイヤ 2 中継の場合は，フレームを受信した VLAN と送信する VLAN は一致します。

表 4-33 VLAN ごとのポート振り分け動作

動作分類	情報元
レイヤ 2 中継	フレームを受信した VLAN ごとに振り分け
IP レイヤ中継	フレームを受信した VLAN ごとに振り分け
自発送信	送信する VLAN ごとに振り分け

(b) VLAN ごとのポート振り分けの注意事項

VLAN ごとのポート振り分けでは以下の項目に注意してください。

- VLAN ごとのポート振り分けを設定している場合，該当リンクアグリゲーションに直接 IP アドレスを設定することはできません。
- VLAN ごとのポート振り分けを使用するためには PSU がすべて PSU-12，PSU-22，PSU-33，PSU-43，または BSU が BSU-C2 もしくは BSU-S2 である必要があります。その他の PSU，BSU を使用している場合はフレーム内情報によるポート振り分けで動作します。
- ソフトウェアで IP レイヤ中継を行うパケットの内，下記パケットは自発送信として扱われ，送信する VLAN ごとに振り分けられます。
  1. DHCP リクエストパケット
  2. トンネルインタフェースを経由して中継するパケット
  3. 未学習のマルチキャスト経路に対して中継対象となるマルチキャストパケット (ただし，マルチキャスト経路を学習後はハードウェア中継となり，フレームを受信した VLAN ごとに振り分けられ

ます）

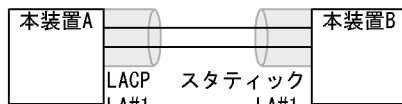
- プライベート VLAN 使用時，ソフトウェアで処理するパケットは下記のように動作します。
  1. Secondary VLAN で受信した IP レイヤ中継を行うパケットは，Secondary VLAN に対応する Primary VLAN ごとに振り分けられます。
  2. Secondary VLAN から自発送信するパケット (レイヤ 2 レベルの制御フレームは除く) は，Secondary VLAN に対応する Primary VLAN ごとに振り分けられます。

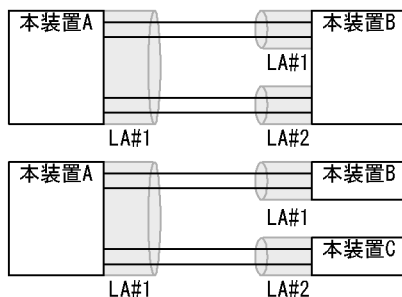
4.6.4 リンクアグリゲーション使用時の注意事項

（1） リンクアグリゲーションが不可能な構成

リンクアグリゲーション構成時には，隣接装置間での設定条件が一致している必要があります。リンクアグリゲーションを構成する装置間は直接接続する必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

図 4-13 リンクアグリゲーションが不可能な構成例

●装置間でモードが異なる場合

この構成を実施したときの動作
・LACP動作によって通信断状態になる。

●装置間でリンクアグリゲーショングループがポイントーマルチポイントになっている場合

この構成を実施したときの動作
・すべてLACPリンクアグリゲーションの場合
　最初にネゴシエーションができたグループ間側だけ動作する。
・すべてスタティックリンクアグリゲーションの場合
　ループ状態になる可能性がある。
・LACP/スタティック混在の場合
　LACPースタティック間で通信断とするためループは回避するが，
　END－END間通信の振り分けが正常に動作しない。

（2） リンクアグリゲーションの構成手順

リンクアグリゲーション構成時には，隣接装置間での設定条件が一致している必要があります。また，「(1) リンクアグリゲーションが不可能な構成」のような構成になっていないことを確認したあとに回線の接続をしてください。

（3） リンクアグリゲーション構成変更の手順

リンクアグリゲーショングループから回線を削除する際は，以下のどれかを実施して該当回線が非運用状態であることを確認してから，コンフィグレーションを変更してください。

- コンフィグレーションで当該回線を disable にする
- 運用コマンドで当該回線を閉塞 (close) する
- 当該ポートのケーブルを抜く

(4) BCU 過負荷時

LACP リンクアグリゲーションモード使用時に BCU が過負荷な状態となった場合，本装置が送受信する LACPDU の廃棄または処理遅延が発生し，タイムアウトのメッセージ出力，一時的な通信断となる場合があります。過負荷状態が頻発する場合は，LACPDU の送信間隔を長くするか，スタティックリンクアグリゲーションを使用してください。

(5) Static モードの離脱ポート数制限機能

Static モードでは，コンフィグレーションコマンド link-aggregation の max-detach-port サブコマンドの指定内容にかかわらず，離脱ポート数制限定義は無効となります。

(6) 異速度混在モードでのフレーム送信時のポート振り分けについて

フレーム送信時のポート振り分けには回線速度の情報は反映しません。例えば，異速度混在モードで 1Gbit/s の回線と 10Gbit/s の回線を使用していても，その回線速度の差はフレーム振り分けには反映しません。

(7) Static モードのスタンバイリンク機能

スタンバイリンクとして選択したポートに対して，test interfaces コマンドで回線テストを実施する場合，以下の注意事項があります。

(a) 当該リンクアグリゲーショングループでは回線テストが終了するまで，運用中のポートに障害が発生した場合でもスタンバイリンクが運用状態に切り替わりません。

(b) 回線テストを実行中に下記コンフィグレーション変更を実施した場合，回線テスト終了後，ポートが閉塞状態のままとなります。ポートを運用状態に戻す場合は free コマンドを使用してください。

- コンフィグレーションコマンド delete link-aggregation <LA ID> で回線テスト実行中の回線を含むリンクアグリゲーショングループを削除した場合
- コンフィグレーションコマンドの delete aggregated-port <Port list> サブコマンドで回線テストを実施しているポートをリンクアグリゲーショングループから削除した場合
- コンフィグレーションコマンドの mode lacp サブコマンドでリンクアグリゲーショングループのモードを LACP に設定した場合

(8) BCU 二重化構成での注意事項【**SB-7800S**】

IP アドレスを付与するインタフェース（レイヤ 2 スイッチ対象外のポート）としてリンクアグリゲーションを使用する場合，インタフェースの MAC アドレスは本装置の MAC アドレスを使用します。BCU 二重化構成での運用時は，本装置の MAC アドレスを運用系，待機系で一致させるためにコンフィグレーションコマンド local-mac-address を設定してください。

4.7　イーサネット使用時の注意事項

4.7.1　禁止トポロジ

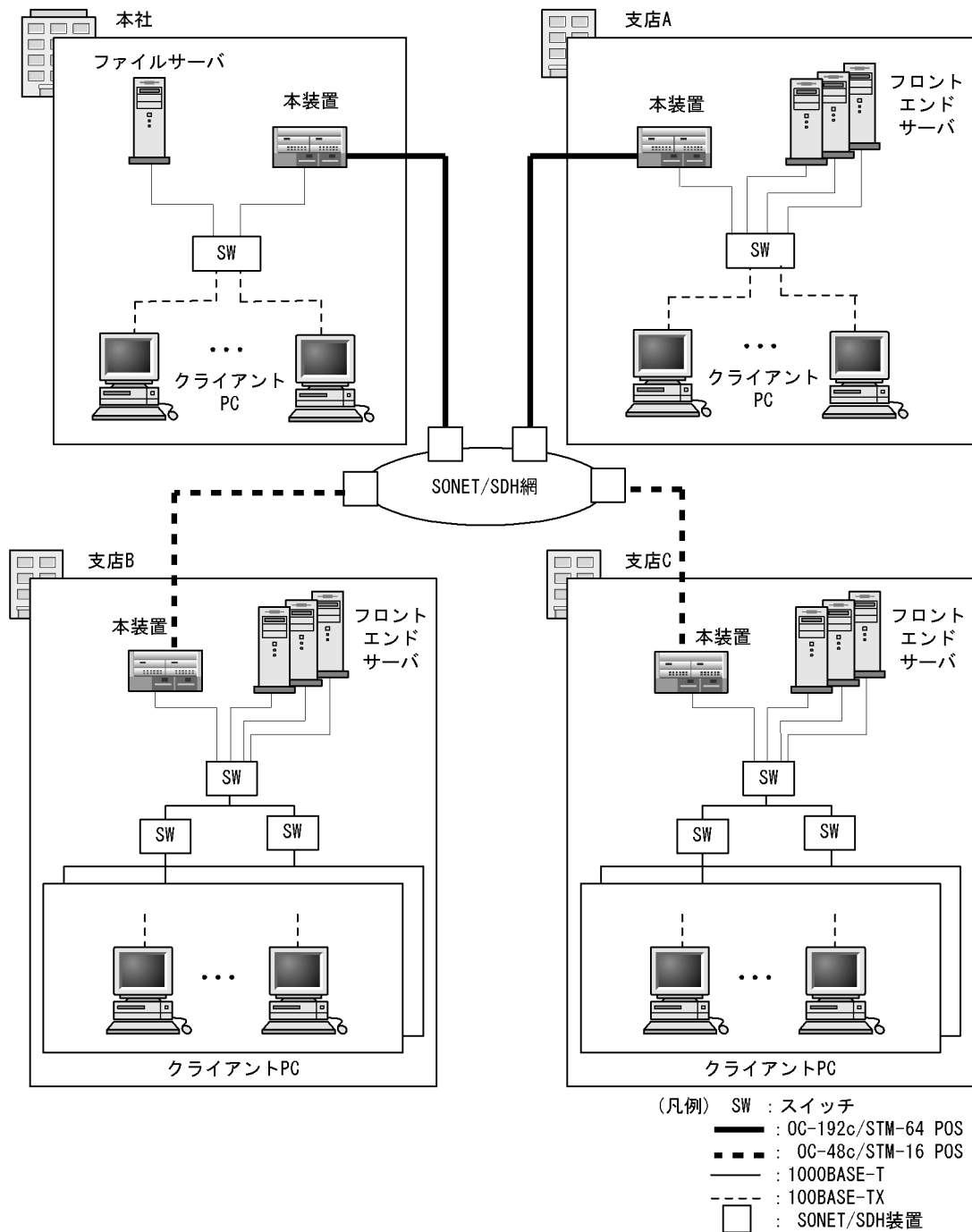
レイヤ 3 スイッチとして使用する場合は，同一ネットワークアドレスを異なる VLAN，RM イーサネットポート（SB-5400S ではリモートマネージメントポート），および NIF 側のイーサネットポートに定義しないでください。同一ネットワークアドレスが定義された場合，通信できないネットワークが発生します。また，異なる VLAN，RM イーサネットポート（SB-5400S ではリモートマネージメントポート），および NIF 側のイーサネットポートは同一ブロードキャストドメインには接続できません。独立したブロードキャストドメインで使用してください。

5 POS（PPP Over SONET/SDH）【SB-7800S】

この章では本装置の POS について説明します。

5.1 ネットワーク構成例

本装置を使用した代表的な POS の構成例を次の図に示します。各ビル間，サーバ間を OC-192c/STM-64 POS および OC-48c/STM-16 POS で接続することによって，従来の OC-3c/STM-1 POS および OC-12c/STM-4 POS よりもサーバ間のパフォーマンスが向上します。

図 5-1　POS の構成例

5.2 物理インタフェース

POS には次のインタフェースがあります。

- OC-192c/STM-64 POS の光ファイバを使用したインタフェース
- OC-48c/STM-16 POS の光ファイバを使用したインタフェース

5.2.1 OC-192c/STM-64 POS

OC-192c/STM-64 POS の光ファイバを使用したインタフェースについて説明します。

(1) 接続仕様

本装置の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

(2) フレームフォーマット

フレームフォーマットを次の図に示します。

図 5-2　フレームフォーマット

SONET/SDHオーバヘッド部

1列
・
・
・
・
9列

SOH(576)
POH(1)
FIXED STUFF(63)
ペイロード(16640)

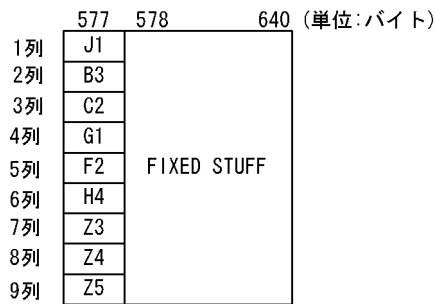
- SOH
  セクションオーバヘッドを示します。セクションオーバヘッドのフォーマットを次の図に示します。

図 5-3　セクションオーバヘッドのフレームフォーマット

（単位：バイト）

	1	2		192	193	194	195		384	385	386		576
1列	A1	A1	・・・	A1	A2	A2	A2	・・・	A2	J0	Z0	・・・	Z0
2列	B1				E1					F1			
3列	D1				D2					D3			
4列	H1	H1	・・・	H1	H2	H2	H2	・・・	H2	H3	H3	・・・	H3
5列	B2	B2	・・・	B2	K1					K2			
6列	D4				D5					D6			
7列	D7				D8					D9			
8列	D10				D11					D12			
9列	S1	Z1	・・・	Z1	Z2	Z2	M1	Z2	・・・	E2			

- POH
  パスオーバヘッドを示します。パスオーバヘッドのフォーマットを次の図に示します。パスオーバヘッドの各バイトの機能を「表 5-1　フレームフォーマットの詳細情報」に示します。

図 5-4　パスオーバヘッドのフレームフォーマット

	577	578　　640（単位：バイト）
1列	J1	FIXED STUFF
2列	B3	
3列	C2	
4列	G1	
5列	F2	
6列	H4	
7列	Z3	
8列	Z4	
9列	Z5	

- ペイロード
  HDLC フレーム（フラグシーケンス，PPP フレーム（アドレス部，制御部，プロトコル識別部，データ部，FCS））が入ります。PPP フレームについては「5.3　PPP」を参照してください。

(3) フレームフォーマットの詳細情報

SONET/SDH 装置との接続の際は，フレームフォーマットの詳細情報を確認の上設定してください。

表 5-1　フレームフォーマットの詳細情報

項目		バイト名称	SONET/SDH(Telecordia / ITU-T) 規格	本装置	
				仕様	デフォルト値
パスシグナルラベル (16 進数)	送信値	C2	16 or CF	スクランブル有効：16 スクランブル無効：CF	16
	P-PLM 障害検出		検出する	検出する	検出する
パスステータス	P-ERDI 転送 (3bit モード)	G1	1 or 3bit モード	1 or 3bit モード	1bit モード
	P-RDI 転送 (1bit モード)				
セクショントレース	送信メッセージトレースモード	J0，Z0	1 オクテット or 16 オクテット or C1 バイト	1 オクテット or C1 バイト	1 オクテット
	1 オクテット (16 進数)	J0	任意の値	00 ～ FF	J0：01 Z0：CC
		Z0	CC	CC	
	C1 バイト (16 進数)	J0	01	01	
		Z0	02,03・・・C0 ※	02,03・・・C0 ※	
	受信メッセージトレースモード	J0	規定なし	1 オクテット or C1 バイト	1 オクテット
パストレース	送信メッセージトレースモード	J1	1 オクテット or 16 オクテット or 64 オクテット	1 オクテット	1 オクテット
	1 オクテット (16 進数)		任意の値	00	00
	受信メッセージトレースモード		規定なし	1 オクテット	1 オクテット
H1 ポインタ内の SS ビット (2 進数)		H1	10	00 or 10	10

注※　Z0 バイトにそれぞれ 02 から 01 ずつ加算し，C0 までの値が入ります。

（4） クロック

本装置では，独立同期および従属同期をサポートしています。

独立同期は WDM（Wavelength Division Multiplexing）装置および，ルータまたはスイッチと接続する場合に指定します。

従属同期は網同期で接続する場合に指定します。なお，従属同期での接続は以下の入力周波数精度の装置としてください。

- 9.95328Gbps ± 4.6ppm 以下（Sonet minimum clock）

本装置のデフォルト値は独立同期です。

（5） CRC 長

本装置では，32 ビットだけサポートしています。相手装置と設定を合わせてください。

（6） スクランブル

スクランブルは，生成多項式：$x^{43}+1$ に従い行われます。スクランブルの対象範囲は，フラグを含むペイロード部分です。ペイロード以外のオーバヘッド部分はスクランブルされません。本装置では，有効または無効を指定できます。その際の C2 バイト（パスシグナルラベル）の値は次の表に示すとおりです。本装置のデフォルト値は有効です。相手装置と設定を合わせてください。

表 5-2　C2 バイトの値

スクランブル	C2 バイト（16 進数）
有効	16
無効	CF

（7） 動作モード

本装置では，SONET および SDH をサポートしています。動作モードを次の表に示します。本装置のデフォルト値は SONET です。相手装置と設定を合わせてください。

表 5-3　動作モード

項目	動作モード	
	SONET	SDH
L-AIS/L-RDI 保護段数	5 回	3 回
H1 ポインタ内の SS ビット（2 進数）	00	10

（8） OC-192c/STM-64 POS 接続時の注意事項

- ループコネクタを接続する場合はクロックを独立同期にしてください。なお，回線テストを実行する場合は，独立同期に変更しなくても実行できます。

5.2.2　OC-48c/STM-16 POS

（1） 接続仕様

本装置の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

（2） フレームフォーマット

フレームフォーマットを次の図に示します。

図 5-5　フレームフォーマット

	SONET/SDHオーバヘッド部			
1列 ・ ・ ・ ・ 9列	SOH(144)	POH(1)	FIXED STUFF(15)	ペイロード(4160)

- SOH
  セクションオーバヘッドを示します。セクションオーバヘッドのフォーマットを次の図に示します。

図 5-6　セクションオーバヘッドのフレームフォーマット

（単位：バイト）

	1	2		48	49	50	51		96	97	98		144
1列	A1	A1	···	A1	A2	A2	A2	···	A2	J0	Z0	···	Z0
2列	B1				E1					F1			
3列	D1				D2					D3			
4列	H1	H1	···	H1	H2	H2	H2	···	H2	H3	H3	···	H3
5列	B2	B2	···	B2	K1					K2			
6列	D4				D5					D6			
7列	D7				D8					D9			
8列	D10				D11					D12			
9列	S1	Z1	···	Z1	Z2	Z2	M1	Z2	···	E2			

- POH
  パスオーバヘッドを示します。パスオーバヘッドのフォーマットを次の図に示します。パスオーバヘッドの各バイトの機能を「表 5-4　フレームフォーマットの詳細情報」に示します。

図 5-7　パスオーバヘッドのフレームフォーマット

（単位：バイト）

	145	146 … 160
1列	J1	FIXED STUFF
2列	B3	
3列	C2	
4列	G1	
5列	F2	
6列	H4	
7列	Z3	
8列	Z4	
9列	Z5	

- ペイロード
  HDLC フレーム（フラグシーケンス，PPP フレーム（アドレス部，制御部，プロトコル識別部，デー

タ部，FCS)）が入ります。PPP フレームについては「5.3　PPP」を参照してください。

(3) フレームフォーマットの詳細情報

SONET/SDH 装置との接続の際は，フレームフォーマットの詳細情報を確認の上設定してください。

表 5-4　フレームフォーマットの詳細情報

項目		バイト名称	SONET/SDH(Telecordia / ITU-T) 規格	本装置	
				仕様	デフォルト値
パスシグナルラベル (16 進数)	送信値	C2	16 or CF	スクランブル有効：16 スクランブル無効：CF	CF
	P-PLM 障害検出		検出する	検出する	検出する
パスステータス	P-ERDI 転送 (3bit モード)	G1	1 or 3bit モード	1 or 3bit モード	1bit モード
	P-RDI 転送 (1bit モード)				
セクショントレース	送信メッセージトレースモード	J0，Z0	1 オクテット or 16 オクテット or C1 バイト	1 オクテット or C1 バイト	1 オクテット
	1 オクテット (16 進数)	J0	任意の値	00 〜 FF	J0：01 Z0：CC
		Z0	CC	CC	
	C1 バイト (16 進数)	J0	01	01	
		Z0	02,03・・・C0 ※	02,03・・・30 ※	
	受信メッセージトレースモード	J0	規定なし	1 オクテット or C1 バイト	1 オクテット
パストレース	送信メッセージトレースモード	J1	1 オクテット or 16 オクテット or 64 オクテット	1 オクテット	1 オクテット
	1 オクテット (16 進数)		任意の値	00	00
	受信メッセージトレースモード		規定なし	1 オクテット	1 オクテット
H1 ポインタ内の SS ビット (2 進数)		H1	10	00 or 10	10

注※　Z0 バイトにそれぞれ 02 から 01 ずつ加算し，30 までの値が入ります。

(4) クロック

本装置では，独立同期および従属同期をサポートしています。

独立同期は WDM（Wavelength Division Multiplexing）装置および，ルータまたはスイッチと接続する場合に指定します。

従属同期は網同期で接続する場合に指定します。なお，従属同期での接続は以下の入力周波数精度の装置としてください。

- 2.48832Gbps ± 20ppm 以下（Sonet minimum clock）

本装置のデフォルト値は独立同期です。

（5） CRC 長

本装置では，16 ビットおよび 32 ビットをサポートしています。本装置のデフォルト値は 16 ビットとなります。相手装置と設定を合わせてください。

（6） スクランブル

スクランブルは，生成多項式：$x^{43}+1$ に従って行われます。スクランブルの対象範囲は，フラグを含むペイロード部分です。ペイロード以外のオーバヘッド部分はスクランブルされません。本装置では，有効または無効を指定できます。その際の C2 バイト（パスシグナルラベル）の値は次の表に示すとおりです。本装置のデフォルト値は無効です。相手装置と設定を合わせてください。

表 5-5　C2 バイトの値

スクランブル	C2 バイト（16 進数）
有効	16
無効	CF

（7） 動作モード

本装置では，SONET および SDH をサポートしています。次の表に動作モードを示します。本装置のデフォルト値は SONET となります。相手装置と設定を合わせてください。

表 5-6　動作モード

項目	動作モード	
	SONET	SDH
L-AIS/L-RDI 保護段数	5 回	3 回
H1 ポインタ内の SS ビット（2 進数）	00	10

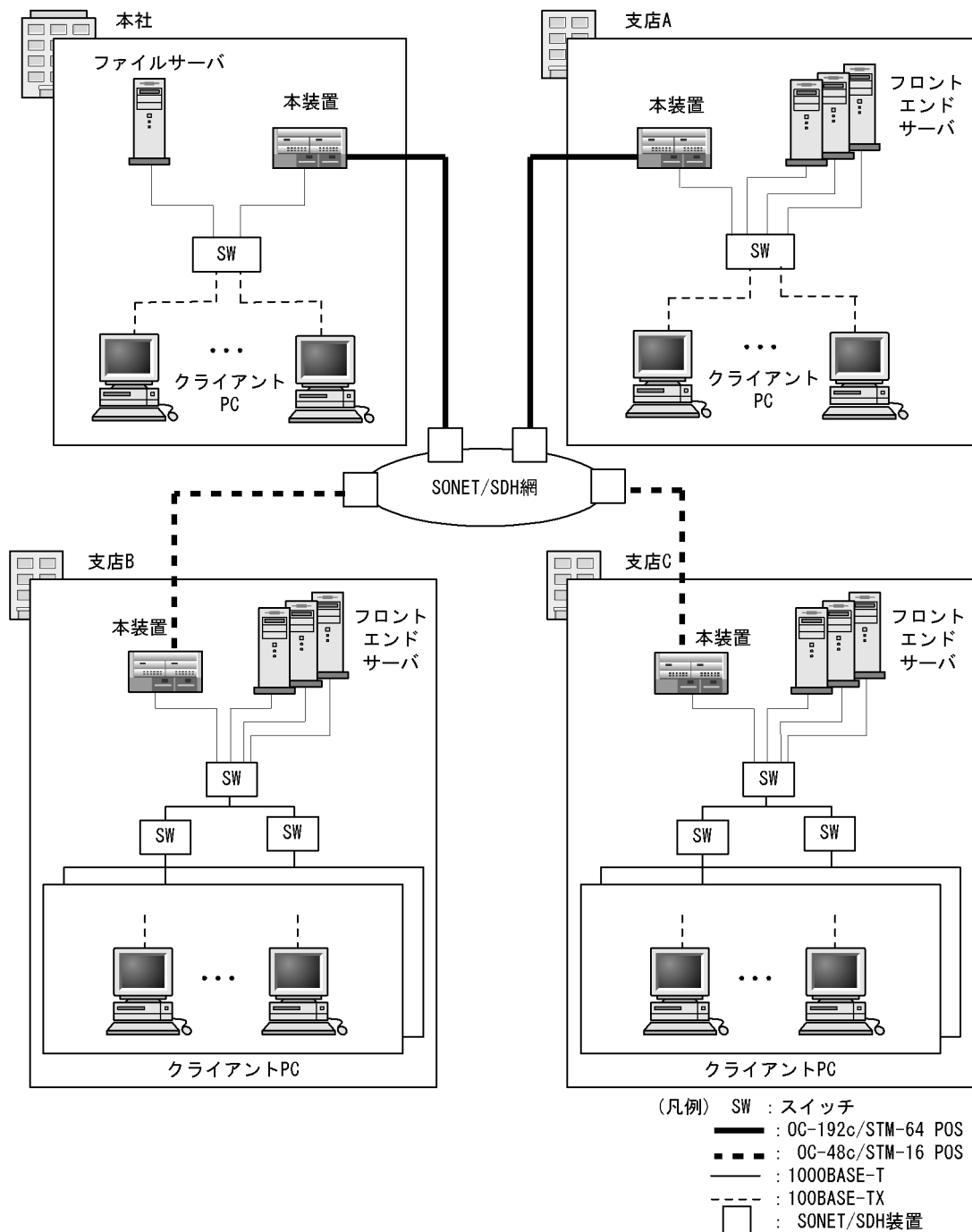
（8） OC-48c/STM-16 POS 接続時の注意事項

- ループコネクタを接続する場合はクロックを独立同期にしてください。なお，回線テストを実行する場合は，独立同期に変更しなくても実行できます。
- マニュアル「ハードウェア取扱説明書」に示す SFP 以外を使用した場合の動作は保証できません。

5.3 PPP

5.3.1 PPP 概説

PPP(Point-to-Point Protocol) は，WAN(Wide Area Network，広域網) などの 2 点間接続のデータ通信で広く利用されているプロトコルです。本装置では，OC-192c/STM-64 POS および OC-48c/STM-16 POS のデータ通信で PPP を使用します。PPP は，1 本のデータリンク上で IP，IPv6，OSI(IS-IS だけで使用) をカプセル化して転送できます。PPP を使用したネットワーク構成例を次の図に示します。

図 5-8　PPP を使用したネットワーク構成例

PPP は大きく分けて次の三つの機能があります。

- 自局と相手局間のデータリンクレイヤレベルのコネクション確立／切断 (LCP)
- 自局と相手局間のネットワークレイヤレベルのコネクション確立／切断 (NCP)
- データのカプセル化（データに PPP ヘッダを付加／削除）

5.3.2　データリンクコネクション

Link Control Protocol(LCP) によって，データリンクレベルでコネクションを確立，切断，管理します。

LCP のサービスは次の三つに分類できます。

- リンク設定 (リンクレベルの初期設定オプションのネゴシエーションおよびリンク確立)
- リンク切断 (PPP のリンク切断)
- リンクメンテナンス (リンク管理および PPP リンクのエラー検出)

LCP は相手局とのリンク状態をモニタリングし，回線品質を検証するオプション機能を持っており，本装置はこれをサポートしています。

5.3.3 ネットワークコネクション

Network Control Protocol(NCP) はネットワークレベルでコネクションを確立，切断，管理します。NCP プロトコルはネットワークレイヤプロトコルごとにあり，本装置では次に示す NCP プロトコルをサポートしています。

- IP に対応する IPCP(IP Control Protocol)
- IPv6 に対応する IPV6CP(IP Version 6 Control Protocol)
- OSI に対応する OSINLCP(OSI Network Layer Control Protocol)

これらの NCP プロトコルは一つのデータリンクコネクション上で多重化されます。

5.3.4 カプセル化

データフォーマットはフラグシーケンスに始まり，アドレス部，制御部，プロトコル識別部，データ部，FCS，そして最後にフラグシーケンスで終わります。PPP でカプセル化したデータフォーマットを次の図に示します。

図 5-9 PPP でカプセル化したデータフォーマット

Flag(1)	Address(1)	Control(1)	Protocol(2)	データ※	FCS(2 or 4)	Flag(1)

( )内の数字はフィールド長を示す(単位はオクテット)。

注※ 最大長は9216オクテットになる。

PPP のカプセル化時の，PPP フレームフォーマットと PPP プロトコルフィールドの値を「表 5-7 PPP フレームフィールドの値」および「表 5-8 PPP プロトコルフィールドの値」に示します。

表 5-7 PPP フレームフィールドの値

フィールド名	値 (16 進数)
Flag	7E 固定
Address	FF 固定
Control	03 固定
Protocol	カプセル化対象とするデータのプロトコル種別に対応する値が入ります。プロトコル種別と値の対応は「表 5-8 PPP プロトコルフィールドの値」を参照してください。
FCS	2 オクテットまたは 4 オクテットの FCS

表 5-8　PPP プロトコルフィールドの値

プロトコル種別			値 (16 進数)
分類	プロトコル		
PPP 制御パケット	LCP		C021
	NCP	IP Control Protocol	8021
		IP Version 6 Control Protocol	8057
		OSI Network Layer Control Protocol	8023
上位レイヤパケット	IP		0021
	IPv6		0057
	OSI		0023

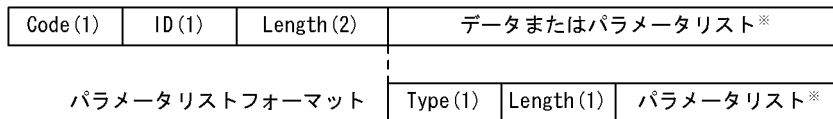
5.3.5　PPP 制御パケット

LCP，NCP の中継プロトコルごとの制御プロトコルで取り扱うパケットを PPP 制御パケットと呼びます。PPP パケットのプロトコルフィールドが LCP，NCP の各制御プロトコルを示す値の場合，PPP パケットのデータ部の内容は PPP 制御パケットになります。PPP 制御パケットフォーマットを次の図に示します。PPP 制御パケットを構成する各フィールドの内容を「表 5-9　PPP 制御パケットの各フィールドの内容」に示します。

図 5-10　PPP 制御パケットフォーマット

Code (1)	ID (1)	Length (2)	データまたはパラメータリスト※

パラメータリストフォーマット

Type (1)	Length (1)	パラメータリスト※

( ) 内の数字はフィールド長を示す (単位はオクテット)。

注※　最大長は，制御パケット種別によって異なる。

表 5-9　PPP 制御パケットの各フィールドの内容

フィールド名	値 (16 進数)
Code	制御パケットの種別
ID	PPP 制御パケットの識別子。Request と Reply の対応づけに使用します。
Length	PPP 制御パケット長。Code からパラメータリストフィールドの最後尾までです。
データまたはパラメータリスト	PPP 制御パケットごとに関連データを格納するフィールド。パラメータリストは，Configure-RQ/Ack/Nak/Rej パケットにあり，「表 5-11　パラメータリスト」に示すパラメータが一つまたは複数個格納されます。

PPP 制御パケットの機能を次の表に示します。

表 5-10　PPP 制御パケットの機能

機能および適用プロトコル	パケット名	Code 値 (16 進数)	ID 値	役割
リンク設定 LCP，IPCP，IPV6CP，OSINLCP	Configure-RQ	01	任意の値	PPP のリンク接続要求パケット。相手局に自局の受信条件を通知。データフィールドにパラメータリストを格納します。
	Configure-Ack	02	Configure-RQ に等しい値	受信 Configure-RQ に対する Ack パケット。相手局から通知された受信条件で接続できる場合は本パケットで応答します。データフィールドにパラメータリストを格納します。
	Configure-Nak	03	Configure-RQ に等しい値	受信 Configure-RQ に対する Nak パケット。相手局から通知された受信条件で接続できず，受信条件の変更を求める場合の応答です。データフィールドにパラメータリストを格納します。
	Configure-Rej	04	Configure-RQ に等しい値	受信 Configure-RQ に対する Reject パケット。相手局から通知された受信条件で接続できず，受信条件の撤回を求める場合の応答です。データフィールドにパラメータリストを格納します。
リンク切断 LCP，IPCP，IPV6CP，OSINLCP	Terminate-RQ	05	任意の値	PPP のリンク切断要求パケット。データフィールドはありません。
	Terminate-Ack	06	Terminate-RQ に等しい値	PPP のリンク切断要求に対する ACK パケット。PPP にはリンク切断要求に対する拒否パケットはありません。データフィールドはありません。
リンクメンテナンス LCP	Echo-RQ	09	任意の値	相手先に対する折り返し要求パケット。このパケットを受信した局は Echo-Reply で応答しなければなりません。データフィールド内容はマジックナンバー※1 と任意のデータ※2 です。
	Echo-Reply	0a	Echo-RQ に等しい値	Echo-RQ に対する Reply パケット。データフィールド内容は Echo-RQ パケットです。
	Discard-RQ	0b	任意の値	相手局に対する廃棄要求パケット (受信した局はこのパケットを廃棄しなければなりません)。データフィールドの内容は任意のデータです。本装置はこのパケットを送信しませんが，受信はできます。
	Identification	0c	任意の値	文字列を使用して自分自身を相手局に認識させるパケット。データフィールドの内容はマジックナンバーと任意の文字列。本装置はこのパケットを送信しませんが，受信はできます。
	Time-Remaning	0d	任意の値	PPP のリンクを一定期間で終了する予定を相手に伝えるパケット。データフィールドの内容はマジックナンバーとリンクの残り時間です。本装置はこのパケットを送信しませんが，受信はできます。
未知 Code パケット拒否 LCP，IPCP，IPV6CP，OSINLCP	Code-Rej	07	任意の値	受信した PPP 制御パケットの Code 値に認識できないものがあった場合の応答です。データフィールドの内容は認識不能なパケットです。

機能および適用プロトコル	パケット名	Code 値 (16 進数)	ID 値	役割
未知プロトコルパケット拒否 LCP	Protocol-Rej	08	任意の値	受信した PPP パケットにサポートしていないプロトコルのパケットがカプセル化されている場合の応答です。データフィールド内容は未サポートパケットです。

注※ 1

ループバック検出用の乱数。

注※ 2

本装置が送信する Echo-RQ には，128 オクテットのデータが付きます。データ内容は，次に示す文字列のアスキーコードの繰り返しになります。
** △ THE △ QUICK △ BROWN △ FOX △ JUMPS △ OVER △ THE △ LAZY △ DOG.123456789 △ **(△はブランク)

本装置がサポートする LCP，IPCP，IPV6CP，OSINLCP それぞれについてパラメータリストを次の表に示します。パラメータリストはこれらのプロトコルの Configure-RQ，Configure-Ack，Configure-Nak，Configure-Rej のデータフィールド部分に格納されます。

表 5-11　パラメータリスト

プロトコル種別	Type (16 進数)	Length	パラメータ・データ		備考
			Data 長	内容	
LCP	01	4	2	MRU(最大受信ユニット) 長	○
	02	6	4	ACC マップ (非同期制御キャラクタマップ)	-
	03	4 以上	2 以上	認証プロトコル識別子など	-
	04	8	2	品質監視プロトコル ID(RFC1333 版，c025(16 進数))	-
			4	品質監視プロトコルパケット送信間隔 (単位＝ 1/100 秒)	-
	05	6	4	マジックナンバー	○
	06	6	4	品質監視パケット (RFC1172 版) の送信間隔 (マイクロ秒単位)	-
	07	2	0	パラメータ・データなし。 このパラメータリストはプロトコルフィールド圧縮を意味します。	-
	08	2	0	パラメータ・データなし。 このパラメータリストは Address/Control 圧縮を意味します。	-
	09	2	0	パラメータ・データなし。 このパラメータリストは 32 ビット CRC を意味します。	-
IPCP	01	10	4	自 IP アドレス	-
			4	相手 IP アドレス	-
	02	4 以上	2 以上	IP 圧縮プロトコル識別子など	-
	03	6	4	自 IP アドレス	○
IPV6CP	01	10	8	インタフェース識別子	○

プロトコル種別	Type (16 進数)	Length	パラメータ・データ		備考
			Data 長	内容	
	02	4 以上	2 以上	IPv6 圧縮プロトコル識別子など	-
OSINLCP	01	3	1	Align-NPDU(PPP ヘッダと OSI パケットとの間の Alignment を設定)	-

(凡例) ○：サポート　-：未サポート
注　パラメータの詳細については該当の RFC を参照してください。

5.3.6 PPP 関係タイマ値，リトライ回数

本装置がサポートする PPP のイベント検出項目と関連するコンフィグレーションのタイマ値およびリトライ回数を次の表に示します。

表 5-12　PPP のイベント検出項目と関連するタイマ値およびリトライ回数

機能および適用プロトコル	PPP のイベント項目	動作時間 (デフォルト値)	関連するコンフィグレーションのタイマ値，リトライ回数
リンク設定 LCP NCP※1	相手局無応答時間	22 秒	retry_timer max_configure
	ネゴシエーション未収束検出時間	数秒以下※2	max_failure
リンク切断 LCP NCP※1	相手局無応答時の切断時間	6 秒	retry _timer max _terminate
リンクメンテナンス LCP	通信中の品質監視間隔	21 秒	echo_trial_times
	通信中の障害検出時間	6 秒	echo_success_times echo_interval

注※1　本装置がサポートする NCP は IPCP，IPV6CP，OSINLCP です。
注※2　厳密には「図 5-13　ネゴシエーション未収束シーケンス例」に示す動作シーケンスを完了するまでの時間であり，相手の応答時間に依存しますが，通常は，即時に応答を返すため，数秒以内でシーケンスが完了します。

本装置では，コンフィグレーションによってタイマ値，リトライ回数を変更できます。本装置がサポートする PPP コンフィグレーションのタイマ値およびリトライ回数の一覧を次の表に示します。

表 5-13　PPP コンフィグレーションのタイマ値およびリトライ回数の一覧

PPP コンフィグレーション	設定値 (デフォルト値)	役割
retry _timer	1 ～ 10 (2) 秒	PPP のリンク設定，リンク切断フレームの送信間隔。リンク設定時に PPP 制御パケットの取りこぼしがある場合などにリンク設定時間を短くして再試行待ち時間を縮められます。
max _configure	1 ～ 255 (10) 回	リンク設定要求フレームの送信リトライ回数
max _terminate	1 ～ 3 (2) 回	リンク切断要求フレームの送信リトライ回数
max_failure	1 ～ 255 (5) 回	PPP 接続条件が収束しないとみなすリトライ回数

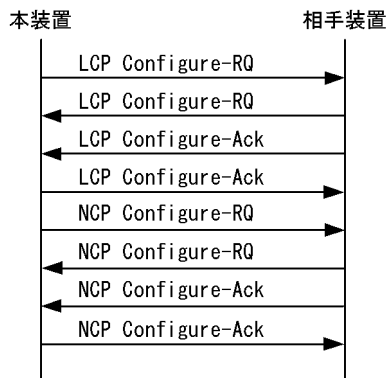
PPP コンフィグレーション	設定値 （デフォルト値）	役割
echo_trial_times	1 ～ 10 (7) 回	リンク品質監視パケットによる品質判定の試行回数。あらかじめ回線品質が悪いことがわかっているシステムや，代替ルートがない WAN 回線を適用するケースなどで，回線品質「悪」検出の感度を鈍くできます。
echo_success_times	1 ～ 10 (6) 回	品質 OK/NG を判断する品質判定試行回数の基準値 (echo success times 以上品質 OK であれば回線品質は良いと判定する)。あらかじめ回線品質が悪いことがわかっているシステムや，代替ルートがない WAN 回線を適用するケースなどで，回線品質「悪」検出の感度を鈍くできます。
echo_interval	0 ～ 255 (3) 秒	回線品質監視パケットの送信間隔。相手局の性能の問題などで，試行間隔を開けなければならない場合などに試行間隔を伸ばせます。

(1) リンク設定時のタイマ

PPP のリンク設定時のタイマについて説明します。

(a) 正常なリンク設定

PPP リンク設定正常シーケンス例を次の図に示します。PPP は，LCP というレイヤと NCP というレイヤに分かれており，各レイヤについて自局／相手局間で Configure-RQ と Configure-Ack の送受信が完了して PPP がオープン状態に入ります。

図 5-11 PPP リンク設定正常シーケンス例

(b) リンク設定時相手無応答検出

PPP リンク設定時，自局からの Configure-RQ 送信に対して，Configure-Ack などの相手局からの応答がない場合に，一定間隔で Configure-RQ の送信をリトライし，リトライアウト発生契機に「接続相手局無応答」の障害を検出します。接続相手局無応答障害検出シーケンス例を次の図に示します。このシーケンスは LCP，NCP で共通です。

関連タイマ値，リトライ回数

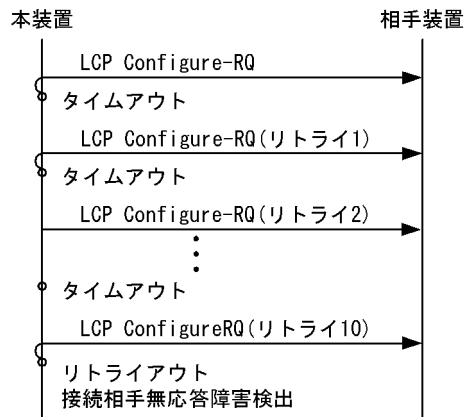
retry_timer：Configure-RQ 送信リトライ間隔，デフォルト値 2 秒

max_configure：Configure-RQ 送信リトライ回数，デフォルト値 10 回

相手局無応答検出時間

(retry_timer) × (max_configure+1)

したがって，デフォルト値使用時は 22 秒。

図 5-12　接続相手無応答障害検出シーケンス例

(c)　ネゴシエーション未収束検出

接続相手との接続条件が収束しないため接続できない場合に，ネゴシエーション・ループの発生を抑える目的から，PPP は「接続相手と接続条件が合わない」と判断する基準値を持っています。この値は次に示す二つのケースで使用されます。

1. 自局が送信した Configure-RQ に対し，接続相手局が拒否パケット (Configure-Nak/Configure-Rej) を送信してくる場合。
2. 接続相手局が送信してくる Configure-RQ に対し，自局が拒否パケット (Configure-Nak/Rej) を送信する場合。ただし，本装置はある構成オプションに対して Configure-Nak を max_failure 分送信してもネゴシエーション未収束を検出せず，Configure-Nak で送信していた構成オプションを付加した Configure-Rej を送信します。

これらのケースについて，ネゴシエーション未収束シーケンス例を次の図に示します。このシーケンスは LCP，NCP で共通です。

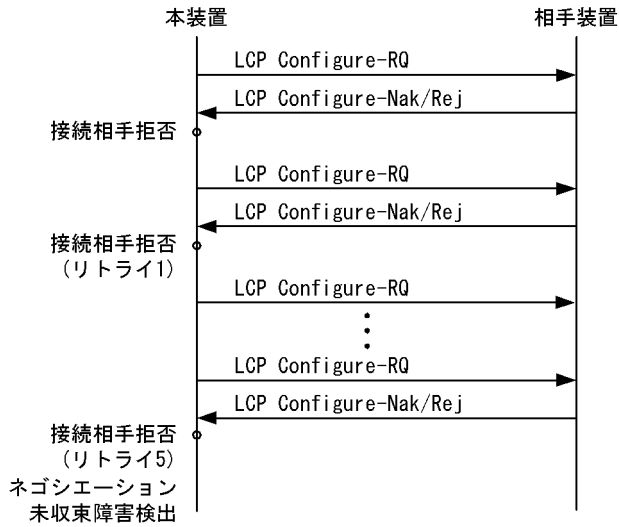
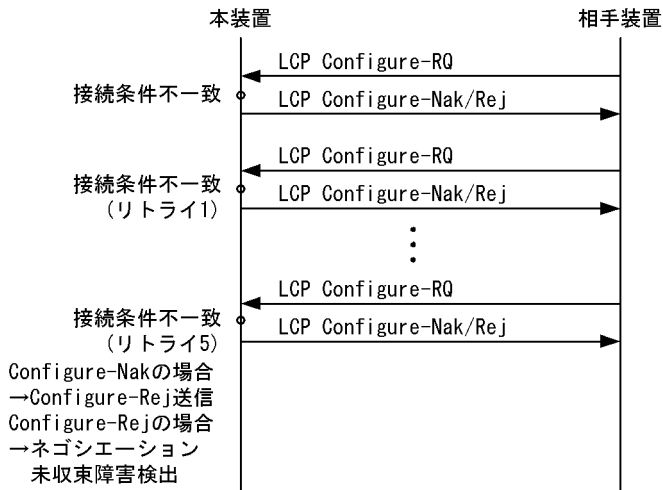
また，1，2 のシーケンスが同時に発生した場合 (Configure-Nak/Configure-Rej を送信し，受信しているようなシーケンス) でも送受信側それぞれ独立にカウントします。

関連タイマ値，リトライ回数

max_failure：Configure-Nak/Configure-Rej 送信リトライ回数です。受信の場合もこの回数で，「ネゴシエーション未収束検出」とします。デフォルト値 5 回です。

ネゴシエーション未収束検出時間

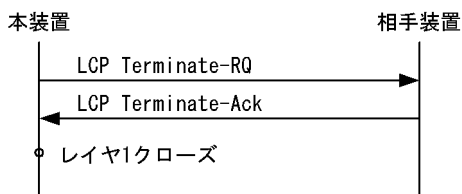
通常，相手局は認められない Configure-RQ を受信したらすぐに Configure-Nak/Rej を，また，Configure-Nak/Rej を受信したらすぐに Configure-RQ を送信するため，ネゴシエーション未収束を検出する時間は数秒以下です。

図 5-13　ネゴシエーション未収束シーケンス例

（2） リンク切断時のタイマ

PPP のリンク切断時のタイマについて説明します。

（a） 正常なリンク切断 (close コマンドなどによる切断)

PPP リンク切断正常シーケンス例を次の図に示します。

図 5-14　PPP リンク切断正常シーケンス例〔PPP 関係タイマ値，リトライ回数〕

PPP は，LCP だけ Terminate-RQ を送信し，Terminate-RQ に対する Terminate-Ack の受信が完了してから，レイヤ 1 に対するクローズ要求を発行します。正常なリンク切断時（close コマンドなどによる切断）は，NCP の Terminate-RQ を送信しないで NCP を切断します。NCP は，該当するネットワークレイヤプロトコルコンフィグレーションが無効になった場合，Terminate-RQ を送信します。

(b) リンク切断時，接続相手無応答検出

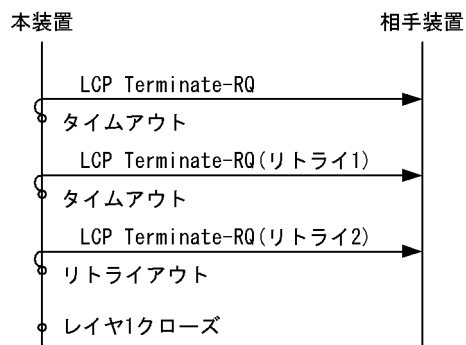
PPP リンク切断時，自局からの Terminate-RQ 送信に対して Terminate-Ack の応答がない場合に，一定間隔で Terminate-RQ の送信をリトライし，リトライアウト発生を契機として下位レイヤのクローズ要求を発行します。リンク切断時接続相手局無応答シーケンス例を次の図に示します。

関連タイマ値，リトライ回数

retry_timer : Terminate-RQ 送信リトライ間隔です。デフォルトは 2 秒です。
max_terminate : Terminate-RQ 送信リトライ回数です。デフォルト値は 2 回です。

相手無応答検出時間

(retry_timer) × (max_terminate ＋ 1)
デフォルト値を使用すると 6 秒になります。

図 5-15　リンク切断時接続相手無応答シーケンス例

(3) リンク品質監視のタイマ

本装置は，Echo の送達確認によるリンク品質監視手順をサポートしています。Echo による品質監視について構成情報と障害検出時間の関係をまとめます。

リンク品質監視は一定間隔でリンク上を流れる固定トラフィックになるので，契約帯域はこれも含めて検討が必要です。リンク品質監視は，Echo-RQ/Echo-Reply によって行い，このパケット長は 142 オクテットです。パケット長は PPP ヘッダ～ FCS の値になります。送信間隔はコンフィグレーションの echo_interval で指定します。なお，本装置は echo_interval 値を 0 に指定すれば，Echo パケットの送信を抑止できます。

系切替が発生すると一時的に相手装置からの Echo-RQ パケットの応答ができない場合があります。それによって，相手装置がリンク品質の低下を検出し，リンク切断を行うことがあります。系切替によるリンク切断を起こさないようにするために，下記の 1. または 2. を実施してください。

1. リンク品質監視の感度を鈍くする。
   PPP リンクの品質監視の感度を鈍くします。本装置と接続する場合，相手装置の ppp コンフィグレーションコマンドの品質監視試行回数 (echo-traial_times) に対する品質監視成功回数 (echo_succes_times) が相対的に小さくなるように設定してください。
2. リンク品質監視を停止する。
   PPP リンク品質監視の実行を停止します。本装置と接続する場合，相手装置の ppp コンフィグレー

ションコマンド品質監視実行間隔 (echo_interval) を 0 に設定してください。

（a） 正常な通信中の品質監視

Echo の送達確認による品質確認を行う場合の正常シーケンス例を次の図に示します。Echo-RQ 送信は "echo_interval" で設定したタイマ値ごとに送信します。

関連タイマ値，リトライ回数

echo_trial_times：Echo-RQ の試行回数です。デフォルトは 7 回です。

echo_success_times：回線品質が良いと判断する Echo-Reply 受信回数です。デフォルト 6 回です。

echo_interval：Echo-RQ の送信間隔です。デフォルトは 3 秒です。

通信中の品質監視間隔

(echo_interval) × (echo_trial times)

このため，デフォルト値を使用したとき，最大 21 秒になります。

図 5-16　Echo の送達確認による品質確認の正常シーケンス例

（b） 障害検出時間

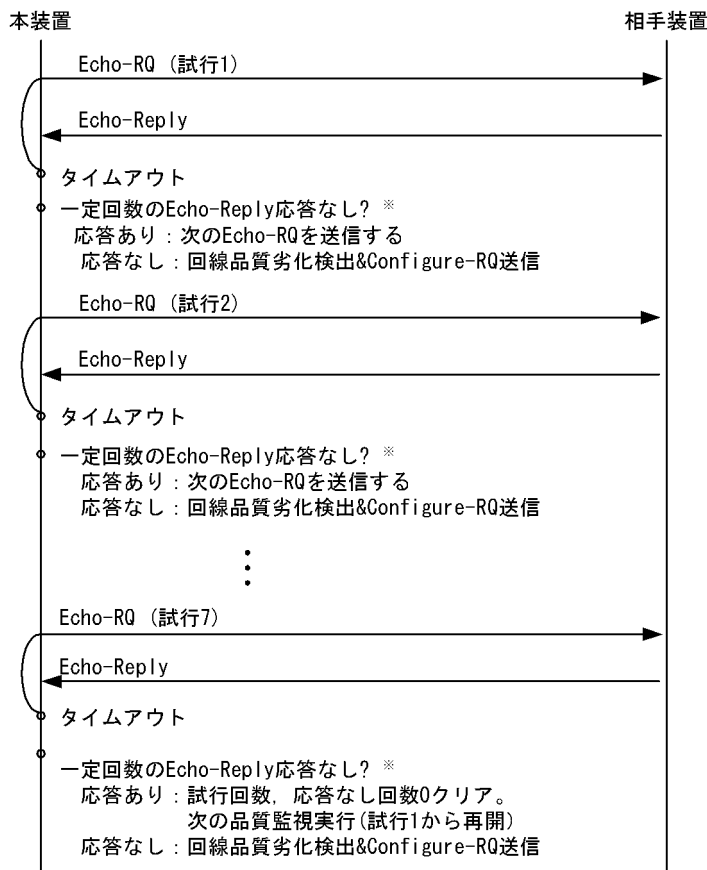
Echo の送達確認による通信中の品質監視を行うことで，回線障害または相手装置無応答等の障害を検出できます。障害が発生してからそれを検出するまでにかかる時間と関連タイマ値およびリトライ回数の関係を示します。

関連タイマ値，リトライ回数

echo_trial_times：Echo-RQ の試行回数です。デフォルトは 7 回です。

echo_success_times：回線品質が良いと判断する Echo-Reply 受信回数です。デフォルト 6 回です。

Echo Interval：Echo-RQ の送信間隔です。デフォルトは 3 秒です。

障害発生後の検出時間

((echo_trial_times)-(echo_success_times) ＋ 1) × (echo_interval)

したがって，デフォルト値を使用した場合，6 秒になります。

関連タイマ，リトライ回数がデフォルト設定時の場合の障害検出シーケンス例を次の図に示します。

図 5-17　障害検出シーケンス例

5.3.7　PPP 障害処理仕様

PPP で障害を検出した場合，PPP のシステムメッセージを表示し，PPP リンクだけ再接続を行います。PPP で検出した障害では物理回線を切断しません。また，LCP で障害を検出した場合は，LCP リンクかつ全 NCP リンクの切断，再接続となり，各 NCP で障害を検出した場合，該当の NCP リンクだけ切断または再接続となります。

6　レイヤ 2 スイッチ

この章では，本装置の機能のうち，OSI 階層モデルの第 2 レイヤでデータを中継するレイヤ 2 スイッチ機能の概要について説明します。

6.1　レイヤ2スイッチ概説

6.1.1　概要

(1) MACアドレス学習とFDB

レイヤ2スイッチはフレームを受信すると送信元MACアドレスをフィルタリング・データベース(FDB)と呼ばれるテーブルに登録します。FDBの各エントリには，MACアドレスとフレームを受信したポートおよび監視事項(エージングタイマ値)が記録されます。フレームを受信するごとに送信MACに対応するFDBのエントリが更新されます。

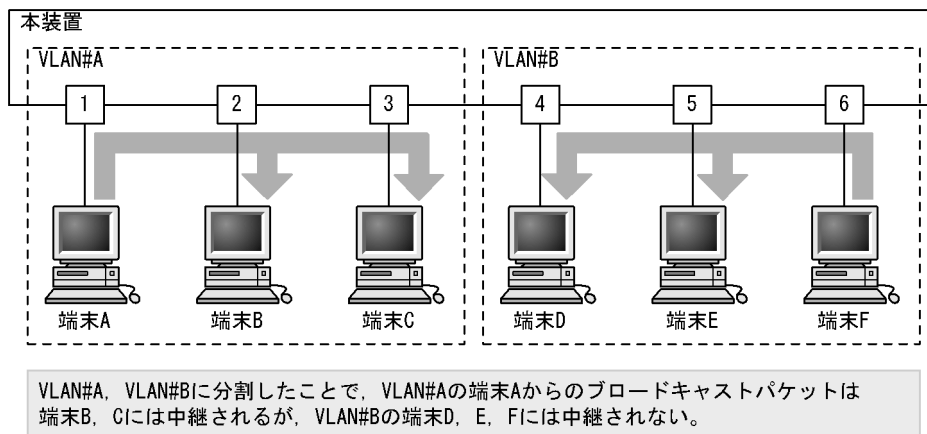
レイヤ2スイッチは，FDBのエントリに従ってフレームのフィルタリングを行います。フレームを受信するとスイッチは宛先MACアドレスとFDB内のMACアドレスを比較します。一致するエントリがないとフレームを受信したインタフェース以外のすべてのインタフェースにフレーム中継を行います。これをフラッディングと呼びます。

宛先MACアドレスに一致するエントリがFDBにあると，スイッチはフレームを受信したインタフェースとFDBのエントリのインタフェースを比較します。インタフェースが同一であればフレームの中継は不要であるため，フレームを廃棄します。インタフェースが異なっていれば，FDBのエントリに示されたインタフェースへフレームを中継します。それ以外のインタフェースへはフレーム中継は行いません。

(2) VLAN

VLANは，スイッチ内を仮想的なグループに分ける機能のことです。スイッチ内を複数のVLANにグループ分けすることによってブロードキャストドメインを分割します。これによって，ブロードキャストフレームの抑制や，セキュリティの強化を図ることができます。

VLANの概要を次の図に示します。VLAN#AとVLAN#Bの間ではブロードキャストドメインが分割されるため，フレームが届くことはありません。

図6-1　VLANの概要

(3) スイッチポートとルータポート

本装置のポートには，VLANに所属するポートとして使用するスイッチポートと，VLANに所属せず単独のポートとして使用するルータポートの2種類があります。

これらのポートの使い方について，次に示します。

(a) スイッチポート

VLAN に所属して使用するポートをスイッチポートと呼びます。VLAN の Untagged ポートまたは Tagged ポートとして設定します。

装置のデフォルトのコンフィグレーションではデフォルト VLAN だけが存在し，すべてのイーサネットのポートがスイッチポートです。

(b) ルータポート

VLAN に所属せず単独のポートで主にレイヤ 3 の機能を使用するポートをルータポートと呼びます。次の表に示す設定をしたポートがルータポートになります。

表 6-1　ルータポートの設定

ルータポート	設定
イーサネット	コンフィグレーションコマンド line（イーサネット）に直接コンフィグレーションコマンド ip を設定
イーサネット （Tag-VLAN 連携）	コンフィグレーションコマンド line（イーサネット）に Tag-VLAN 連携機能（コンフィグレーションコマンド vlan）を設定
リンクアグリゲーション	リンクアグリゲーションに直接コンフィグレーションコマンド ip を設定
リンクアグリゲーション （Tag-VLAN 連携）	リンクアグリゲーションに Tag-VLAN 連携機能（コンフィグレーションコマンド vlan）を設定
POS	POS のポート

(c) スイッチポートとルータポートの違い

スイッチポートは，VLAN を使用して，レイヤ 2 スイッチ機能およびレイヤ 3 機能を使用できます。

ルータポートは，スイッチポートとして設定している VLAN とは独立のポートして使用できます。NIF の一つのポートおよびリンクアグリゲーションをレイヤ 3 インタフェースとして使用したい場合に，VLAN ID を使用せずに IP アドレスを付与してレイヤ 3 機能などを使用できます。また，Tag-VLAN 連携機能で設定する VLAN ID は，スイッチポートで使用している VLAN の VLAN ID，または別ポートで設定している Tag-VLAN 連携機能の VLAN ID とは無関係に番号を割り当てることができます。

(d) スイッチポートとルータポートのサポート機能

レイヤ 2 スイッチ機能とその関連機能において，ルータポートまたはスイッチポートのどちらかだけしか使用できない機能があります。それぞれのサポート機能を次の表に示します。ルータポートはレイヤ 2 スイッチ機能を使用できない点がスイッチポートとは異なります。

表 6-2　スイッチポート，ルータポートのサポート機能

機能	スイッチポート	ルータポート
イーサネット（line）	○	○
POS	×	○
リンクアグリゲーション	○	○
Tag-VLAN 連携機能	×	○
MAC アドレス学習	○	×
VLAN 機能	○	×
VLAN 拡張機能	○	×

機能	スイッチポート	ルータポート
スパニングツリー	○	×
IGMP snooping，MLD snooping	○	×
GSRP	○	×
IEEE802.1X 機能	○	×

（凡例）○：サポートします。×：サポートしていません。

6.1.2　サポート機能

レイヤ 2 スイッチ機能として，本装置がサポートする機能を次の表に示します。

これらの機能は，組み合わせて利用できる機能とできない機能があります。機能の組み合わせ制限については，次項で説明します。

表 6-3　レイヤ 2 スイッチサポート機能

サポート機能		機能概要
MAC アドレス学習	学習機能	FDB に登録する MAC アドレスの学習機能
	学習数制限機能	学習する最大 MAC アドレス数を制限する機能
	学習の ON/OFF 機能	MAC アドレスの学習を停止する機能
VLAN	ポート VLAN	ポート単位にスイッチ内を仮想的なグループに分ける機能
	プロトコル VLAN	プロトコル単位にスイッチ内を仮想的なグループに分ける機能
	MAC VLAN **【SB-7800S】**	送信元の MAC アドレス単位にスイッチ内を仮想的なグループに分ける機能
	デフォルト VLAN	コンフィグレーションが未設定のときにデフォルトで所属する VLAN
	トンネリング	複数ユーザの VLAN をほかの VLAN に集約して「トンネル」する機能
	アップリンク VLAN	VLAN 内で端末を接続するポート間での通信（レイヤ 2）を遮断する機能
	アップリンクブロック	VLAN 内でアップリンク間の通信（レイヤ 2）を遮断する機能
	プライベート VLAN	複数の VLAN を組み合わせて一つのサブネットを構成する機能
	Tag 変換機能	VLAN のタグを変換して別の VLAN に中継する機能
	未定義フレーム廃棄機能	あらかじめ定義した VLAN の内容と異なる条件のフレームを受信した場合に，受信フレームを破棄する機能です。
	BPDU フォワーディング機能	スパニングツリーを使用しない VLAN で BPDU を中継する機能
	EAPOL フォワーディング機能	IEEE802.1X を使用しない VLAN で EAPOL を中継する機能
	VLAN ごと MAC アドレス	レイヤ 3 インタフェースの MAC アドレスを VLAN ごとに異なるアドレスにする機能
スパニングツリー	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	PVST+	VLAN 単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
IGMP snooping/MLD snooping		レイヤ 2 スイッチで VLAN 内のマルチキャストトラフィック制御機能

6.1.3　レイヤ 2 スイッチ機能と他機能の共存について

レイヤ 2 スイッチ機能と併用する際，共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

なお，これらの表では各機能間の共存関係において，制限のある項目だけを示しています。

表 6-4　MAC アドレス学習での制限事項

<table>
<tr><th>使用したい機能</th><th>制限のある機能</th><th>制限の内容</th></tr>
<tr><td rowspan="3">アドレス学習数制限機能</td><td>802.1X ポート単位認証</td><td rowspan="3">一部制限あり※</td></tr>
<tr><td>802.1X VLAN 単位認証 (静的)</td></tr>
<tr><td>802.1X VLAN 単位認証 (動的)
【SB-7800S】</td></tr>
<tr><td rowspan="3">MAC アドレス学習の ON/OFF 機能</td><td>802.1X ポート単位認証</td><td rowspan="3">共存不可</td></tr>
<tr><td>802.1X VLAN 単位認証 (静的)</td></tr>
<tr><td>802.1X VLAN 単位認証 (動的)
【SB-7800S】</td></tr>
</table>

注※　アドレス学習数制限機能で，制限を超えたときの動作を転送にしているポートが一つでもある場合は，その VLAN で IEEE802.1X 機能を使用できません。アドレス学習数制限機能の制限を超えたときの動作を破棄にしている場合は，IEEE802.1X 機能のポート単位認証を使用できます。

表 6-5　VLAN での制限事項

<table>
<tr><th colspan="2">使用したい機能</th><th>制限のある機能</th><th>制限の内容</th></tr>
<tr><td rowspan="16">VLAN 種別</td><td rowspan="3">ポート VLAN</td><td>VLAN トンネリング</td><td>一部制限あり※1</td></tr>
<tr><td>802.1X ポート単位認証</td><td>一部制限あり※2</td></tr>
<tr><td>802.1X VLAN 単位認証 (動的)
【SB-7800S】</td><td>共存不可</td></tr>
<tr><td rowspan="8">プロトコル VLAN</td><td>デフォルト VLAN</td><td rowspan="8">共存不可</td></tr>
<tr><td>VLAN トンネリング</td></tr>
<tr><td>BPDU フォワーディング</td></tr>
<tr><td>EAPOL フォワーディング</td></tr>
<tr><td>PVST+</td></tr>
<tr><td>802.1X ポート単位認証</td></tr>
<tr><td>802.1X VLAN 単位認証 (静的)</td></tr>
<tr><td>802.1X VLAN 単位認証 (動的)
【SB-7800S】</td></tr>
<tr><td rowspan="5">MAC VLAN
【SB-7800S】</td><td>デフォルト VLAN</td><td rowspan="5">共存不可</td></tr>
<tr><td>VLAN トンネリング</td></tr>
<tr><td>PVST+</td></tr>
<tr><td>802.1X ポート単位認証</td></tr>
<tr><td>802.1X VLAN 単位認証 (静的)</td></tr>
</table>

使用したい機能		制限のある機能	制限の内容
		802.1X VLAN 単位認証 (動的) **【SB-7800S】**	一部制限あり※ 3
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN **【SB-7800S】**	
		Tag 変換機能	
		アップリンク VLAN	
		アップリンクブロック	
		プライベート VLAN	
		PVST+	
		IGMP snooping	
		MLD snooping	
		802.1X VLAN 単位認証 (静的)	
		802.1X VLAN 単位認証 (動的) **【SB-7800S】**	
VLAN 拡張機能	未定義フレーム廃棄機能	802.1X VLAN 単位認証 (動的) **【SB-7800S】**	一部制限あり※ 4
	Tag 変換機能	デフォルト VLAN	共存不可
		PVST+	
		IGMP snooping	
		MLD snooping	
	アップリンク VLAN	デフォルト VLAN	共存不可
		アップリンクブロック	
		プライベート VLAN	
		IGMP snooping	
		MLD snooping	
	アップリンクブロック	デフォルト VLAN	共存不可
		アップリンク VLAN	
		プライベート VLAN	
		IGMP snooping	
		MLD snooping	
	プライベート VLAN	デフォルト VLAN	共存不可
		アップリンク VLAN	
		アップリンクブロック	
		IGMP snooping	
		MLD snooping	
		VRRP	
		IPv4，IPv6 マルチキャスト	
		ポリシールーティング	
	VLAN トンネリング	ポート VLAN	一部制限あり※ 1
		プロトコル VLAN	共存不可

使用したい機能		制限のある機能	制限の内容
		MAC VLAN **【SB-7800S】**	
		IGMP snooping	
		MLD snooping	
		802.1X ポート単位認証	
		802.1X VLAN 単位認証 (静的)	
		802.1X VLAN 単位認証 (動的) **【SB-7800S】**	
	BPDU フォワーディング	プロトコル VLAN	共存不可
		PVST+	
	EAPOL フォワーディング	プロトコル VLAN	共存不可
		802.1X ポート単位認証	
		802.1X VLAN 単位認証 (静的)	
		802.1X VLAN 単位認証 (動的) **【SB-7800S】**	
	VLAN ごと MAC アドレス	プライベート VLAN	共存不可

注※ 1

VLAN トンネリング機能を使用する場合は，ハイブリッドリンクを使用することができません。

注※ 2

Tagged ポートおよびハイブリッドリンクでは，IEEE802.1X 機能のポート単位認証を使用できません。

注※ 3

IEEE802.1X 機能の VLAN 単位認証（動的）は，MAC VLAN の Untagged ポートだけで使用できます。MAC VLAN の Tagged ポートおよびハイブリッドリンクは，自動的に認証除外ポートになります。**【SB-7800S】**

注※ 4

未定義フレーム廃棄機能を使用しているポートがある VLAN では，IEEE802.1X 機能の VLAN 単位認証（動的）を使用できません。**【SB-7800S】**

表 6-6　スパニングツリーでの制限事項

使用したい機能	制限のある機能	制限の内容
シングルスパニングツリー	マルチプルスパニングツリー	共存不可
	GSRP	
PVST+	デフォルト VLAN	共存不可
	プロトコル VLAN	
	MAC VLAN **【SB-7800S】**	
	Tag 変換機能	
	BPDU フォワーディング	
	マルチプルスパニングツリー	
	GSRP	
マルチプルスパニングツリー	シングルスパニングツリー	共存不可
	PVST+	
	ループガード	
	GSRP	

表 6-7　IGMP/MLD snooping での制限事項

使用したい機能	制限のある機能	制限の内容
IGMP snooping	デフォルト VLAN	共存不可
	Tag 変換機能	
	アップリンク VLAN	
	アップリンクブロック	
	プライベート VLAN	
	VLAN トンネリング	
MLD snooping	デフォルト VLAN	共存不可
	Tag 変換機能	
	アップリンク VLAN	
	アップリンクブロック	
	プライベート VLAN	
	VLAN トンネリング	

6.2　MAC アドレス学習機能

6.2.1　概要

本装置は，フレームを宛先 MAC アドレスによって目的のポートへ中継するレイヤ 2 スイッチングを行います。宛先 MAC アドレスによって特定のポートだけに中継することによって，ユニキャストフレームによる無駄なトラフィックを抑止します。

なお，本装置では MAC アドレス学習機能として，本項で説明する基本的な機能のほかに，次の四つの機能をサポートしています。

- 学習機能の ON/OFF 機能
  MAC アドレス学習の実施 / 未実施を指定できるようにする機能。
- アドレス学習数制限機能
  MAC アドレス学習で，学習する最大アドレス数を制限する機能。
- FDB クリア機能
  学習した FDB をクリアする機能。
- スタティックエントリ登録機能
  ユーザが定義で FDB に MAC アドレスを登録する機能。

これら四つの機能については，次項以降を参照してください。

（1） 送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし，送信元 MAC アドレスを学習して FDB(Filtering Data Base) に登録します。登録した MAC アドレスはエージングタイムアウトまで保持し続けます。学習は VLAN 単位に行い，FDB は MAC アドレスと VLAN のペアによって管理します。異なる VLAN であれば同一の MAC アドレスを学習することもできます。

（2） MAC アドレスの移動検出

すでに学習済みの送信元 MAC アドレスを持つフレームを学習時と異なるポートから受信した場合，その MAC アドレスが移動したものと見なして FDB のエントリを再登録 (移動先ポートに関する上書き) します。

（3） 学習 MAC アドレスのエージング

学習したエントリは，エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合はエントリを削除します。これによって，不要な FDB エントリの蓄積を防止します。エージングタイム内にフレームを受信した場合は，エージングタイマを更新しエントリを保持し続けます。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0，10 ～ 1,000,000(秒)
  0 は無限を意味し，エージングしません。
- デフォルト値　　：300(秒)

また，ポートがダウンした場合には FDB 上の該当ポートから学習したエントリを削除します。

（4） MAC アドレス学習によるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングを行います。宛先 MAC アドレスに対応する

FDB エントリを保持している場合，学習したポートだけに中継します。

レイヤ 2 スイッチングの動作仕様を示します。

表 6-8　レイヤ 2 スイッチングの動作仕様

宛先 MAC アドレスの種類	動作概要
学習済みのユニキャスト	学習した受信ポートへ中継します。
未学習のユニキャスト	受信した VLAN に所属する全ポートへ中継します。
ブロードキャスト	受信した VLAN に所属する全ポートへ中継します。
マルチキャスト	受信した VLAN に所属する全ポートへ中継します。 ただし，IGMP snooping，MLD snooping 動作時は snooping 機能の学習結果に従って中継します。

6.2.2　MAC アドレス学習の ON/OFF 機能

MAC アドレス学習を行わない VLAN を設定できます。通常は VLAN 作成時から MAC アドレス学習を行いますが，これを OFF にすることによってその VLAN 上でのダイナミックな MAC アドレス学習を停止します。

学習機能を OFF にすると，それまでのダイナミックに学習済みの MAC アドレスはすべて削除します。この機能は，すべての受信フレームを全ポートにフラッディングしたい場合に有効です。

6.2.3　MAC アドレス学習数制限

（1） MAC アドレス学習数制限

MAC アドレス学習で，学習する最大アドレス数を制限できます。一定数以上の MAC アドレスを FDB に登録しないで，FDB の消費エントリ数をユーザの想定する範囲内に収めるための機能です。MAC アドレス学習数制限を次の表に示します。

表 6-9　MAC アドレス学習数制限

項目	概要
制限数にカウントするアドレス	ダイナミックに学習したアドレス
設定単位	ポート単位
制限値の範囲	0 ～ 100,000 制限数に 0 を指定すると，ダイナミックな学習は行わなくなります。
制限を超えたときの動作	制限を超えて学習対象となるフレームを受信したときの動作は次から選択できます。 • 転送：中継します。 • 廃棄：制限を超えたフレームは廃棄します (MAC 学習もしません)。 制限数の設定を変更するときに，現在の学習数より小さい数字を設定した場合は，エージングを待つか FDB をクリアするコマンドで削除してください。

（2） 注意事項

MAC アドレス学習数制限で，リンクアグリゲーションのポートを指定し，かつ該当リンクアグリゲーションのポートが複数 PSU にわたっていた場合，学習制限に達した直後も該当リンクアグリゲーションのおのおののポートから未学習フレームを同時かつ継続的に受信し続けると，学習制限に達した旨の警告

メッセージが頻発することがあります。PSU 間の FDB 同期処理に伴うものであり，通常運用では数秒から数十秒でメッセージ出力は収まります。

6.2.4　FDB クリア機能

ダイナミックに学習した FDB をクリアすることができます。

クリアする単位として，全 FDB 内容を一括クリアする指定のほかに VLAN 番号を指定することで指定 VLAN として学習した全 MAC アドレスを FDB からクリアします。

また，ポート番号を指定することで指定ポートから学習した MAC アドレスを FDB からクリアします。

6.2.5　スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに，ユーザ指定によってスタティックに MAC アドレスを登録することができます。ユニキャスト MAC アドレスに対して一つの送信先ポートまたはリンクアグリゲーショングループを指定することができます。また，送信先ポートを指定するのではなく " 廃棄 " を指定することもできます。その場合指定の宛先 MAC アドレスのフレームはどのポートにも中継せずに廃棄します。

ユニキャスト MAC アドレスに対してスタティックな登録を行うと，そのアドレスに関してダイナミックな学習は行いません。既に学習済みのエントリは FDB から削除してスタティックエントリを登録します。次の表にスタティックエントリの指定パラメータを示します。

表 6-10　スタティックエントリの指定パラメータ

項番	指定パラメータ	説明
1	宛先 MAC アドレス	ユニキャスト MAC アドレスが指定可能です。
2	VLAN	このエントリを登録する VLAN を指定します。
3	送信先ポート / 廃棄指定	一つのポートまたはリンクアグリゲーショングループ指定が可能です。また，項番 1,2 に該当するフレームを廃棄する指定ができます。

VLAN に IP アドレスを付与して IP 中継を行う場合，VLAN から出力する IP パケットにスタティックエントリが作用します。例えば，中継している IP ユニキャストパケットの宛先 MAC アドレスを指定して該当 VLAN に廃棄指定のエントリを登録すると中継が停止します。

6.2.6　注意事項

（1） MAC アドレス学習の FDB 消費量

MAC アドレス学習では，VLAN に関する特殊機能を使用している場合に一つの MAC アドレスに対し複数の FDB エントリ（H/W リソース）を消費する場合があります。関連機能と FDB 消費量の関係を次の表に示します。なお，FDB 消費量は show psu resources(SB-5400S では show bsu resources) コマンドで確認できます。

表 6-11　MAC アドレス学習の FDB 消費量

機能	FDB エントリ消費
通常の MAC 学習	一つの MAC アドレスに対し 1 エントリ

機能	FDB エントリ消費
アップリンク VLAN	アップリンク VLAN 機能使用時のエントリ消費量は次のとおりです。 • アップリンクポートの設定 設定したポートごとに 1 エントリ • アップリンクポートで学習した MAC 一つの MAC アドレスに対し 1 エントリ • 端末接続ポートで学習した MAC loose モード…一つの MAC アドレスに対し 1 エントリ strict モード…該当 VLAN の [アップリンクポート数＋ 1] のエントリ
アップリンクブロック	アップリンクブロック機能使用時のエントリ消費量は次のとおりです。 • ブロックポートの設定 設定したポートごとに 1 エントリ • ブロックポートで学習した MAC 該当 VLAN の [ブロックポート数＋ 1] のエントリ • 端末接続ポートで学習した MAC 一つの MAC アドレスに対し 1 エントリ
プライベート VLAN	一つの MAC アドレスに対して，その MAC アドレスを学習するプライベート VLAN の Primary VLAN と Secondary VLAN を合計した VLAN 数のエントリ

SB-7800S 使用時，VLAN が複数の PSU をまたがっている場合，一つの MAC アドレスを学習することによってその VLAN を持つすべての PSU で 1 エントリづつ消費します。

7 VLAN

VLAN はスイッチ内を仮想的なグループに分ける機能です。この章では VLAN について説明します。

7.1 VLAN 概説

この節では，VLAN の種類および機能について説明します。

7.1.1 VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 7-1　サポートする VLAN の種類

項目	概要
ポート VLAN	ポート単位に VLAN のグループを分けます。
プロトコル VLAN	プロトコル単位に VLAN のグループを分けます。
MAC VLAN **【SB-7800S】**	送信元の MAC アドレス単位に VLAN のグループを分けます。

7.1.2 Tagged ポートと Untagged ポート

VLAN 内のポート単位に VLAN-Tag の付与を指定できます。VLAN-Tag を付与するポートを Tagged ポート，指定しないポートを Untagged ポートと呼びます。

（1） 同一ポート上の VLAN の混在

VLAN の種類と Tagged ポートおよび Untagged ポートの種類によって，同一ポート上で設定できる VLAN の組み合わせが異なります。同一ポートでの VLAN の組み合わせを次の表に示します。用途に応じて，表に示すポートの種類のどれかで設定します。

表 7-2　同一ポートでの VLAN の組み合わせ

ポートの種類	用途
Untagged ポート	VLAN-Tag を使用せずに一つの VLAN だけを使用するポートです。ポート VLAN の Untagged ポートを一つだけ設定します。
プロトコルポート	プロトコルごとに VLAN を分けるポートです。プロトコル VLAN の Untagged ポートを設定します。
MAC ポート	フレームの送信元 MAC アドレスごとに VLAN を分けるポートです。MAC VLAN の Untagged ポートを設定します。
Tagged ポート	VLAN-Tag で VLAN を分けるポートです。VLAN の種類にかかわらず Tagged ポートを設定します。 Tagged ポートにはポート VLAN の Untagged ポートも同時に設定できます。 Untagged ポートを同時に設定したポートをハイブリッドリンクと呼びます。

ポートの種類ごとの，VLAN の種類と Tagged ポートおよび Untagged ポートの設定の組み合わせを次の表に示します。ポート VLAN の Untagged ポートだけがほかのポート設定と同一のポートで混在できます。

表 7-3　同一ポート上で使用できる VLAN の組み合わせ

ポートの種類	VLAN の種類と Tagged ポートおよび Untagged ポート			
	ポート VLAN Untagged ポート	プロトコル VLAN Untagged ポート	MAC VLAN **【SB-7800S】** Untagged ポート	各種 VLAN 共通 Tagged ポート
Untagged ポート	○	×	×	×
プロトコルポート	○	○	×	×
MAC ポート	○	×	○	×
Tagged ポート	○	×	×	○

（凡例）○：混在できる　×：混在できない

(2) フレーム送信時の VLAN-Tag の扱い

フレーム送信時の VLAN-Tag の扱いは送信するポートの Tagged/Untagged 設定に従って送信します。Tagged ポートの場合は設定された VLAN ID によって VLAN-Tag を付与して送信します。Untagged ポートの場合は VLAN-Tag を付与しないで送信します。

7.1.3　デフォルト VLAN

(1) 概要

本装置では，コンフィグレーションが未設定の状態であっても，装置の起動後すぐにレイヤ 2 中継ができます。このとき，すべてのスイッチポートはデフォルト VLAN と呼ぶ VLAN に属します。デフォルト VLAN は常に存在し，VLAN ID には「1」を使用します。VLAN ID「1」は，装置内で予約番号として扱うため，変更することはできません。また，ID 以外にも，コンフィグレーションで設定できる項目は通常の VLAN とは異なります。

なお，VLAN を設定したポートで，受信したフレームの所属する VLAN が設定した VLAN に一致しない場合にはデフォルト VLAN のフレームとして取り扱います。

(2) デフォルト VLAN から除外するポート

デフォルト VLAN にはコンフィグレーション未設定の状態で自動的にポートが所属しますが，コンフィグレーションによってデフォルト VLAN の自動的な所属から除外する場合があります。次に示すポートはデフォルト VLAN に自動的に所属しなくなります。

- VLAN 1 以外のポート VLAN で Untagged ポートとして設定しているポート
- 未定義フレーム廃棄機能を設定しているポート
- VLAN トンネリング機能を設定した場合の全ポート
- ルータポート

7.1.4　VLAN の優先順位

(1) フレーム受信時の VLAN 判定の優先順位

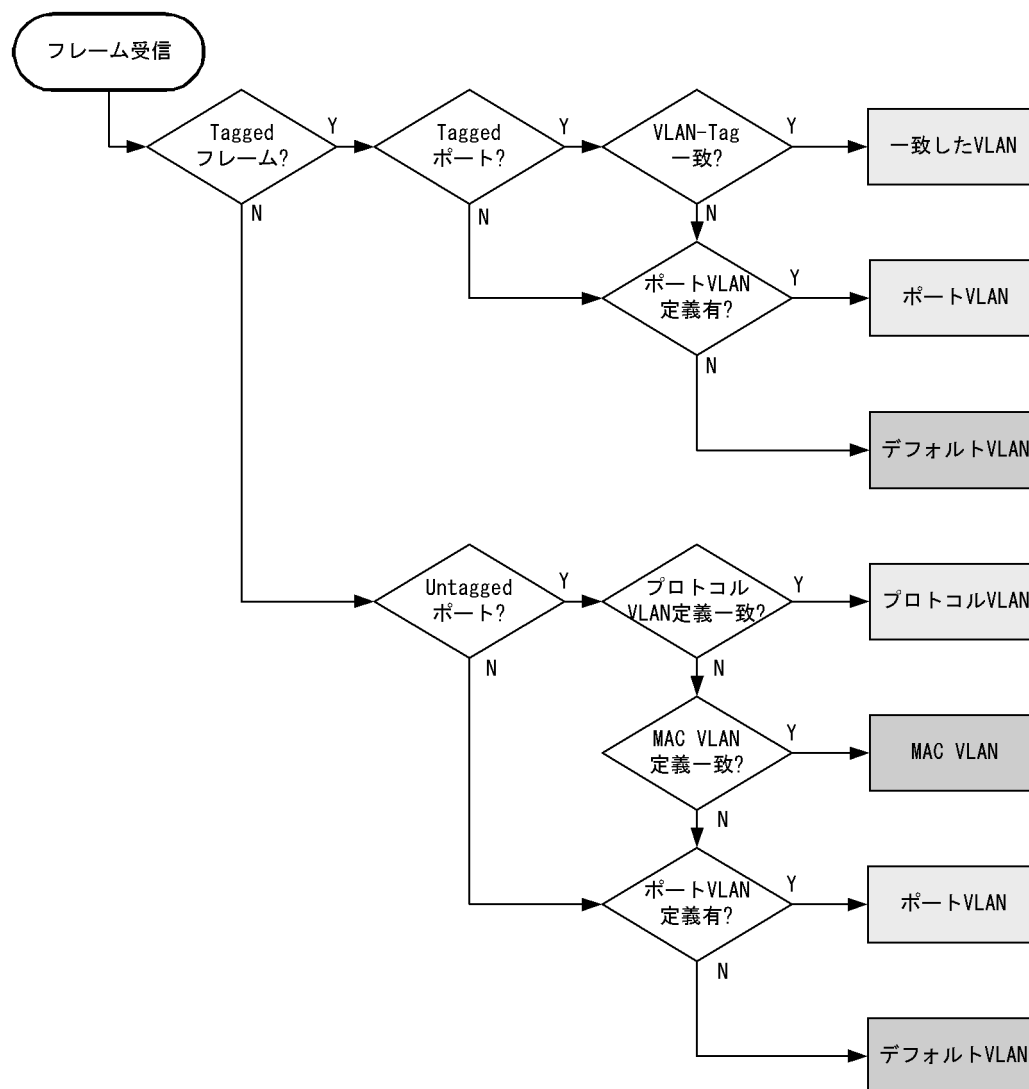
VLAN を設定したポートでフレームを受信した場合，受信したフレームの所属する VLAN の判定を行います。VLAN 判定の優先順位を次に示します。

表 7-4　VLAN 判定の優先順位

ポートの種類	VLAN 判定の優先順位
Untagged ポート	ポート VLAN ＞デフォルト VLAN
プロトコルポート	プロトコル VLAN ＞ポート VLAN ＞デフォルト VLAN
MAC ポート	MAC VLAN ＞ポート VLAN ＞デフォルト VLAN
Tagged ポート	VLAN-Tag ＞ポート VLAN ＞デフォルト VLAN

注 「ポート VLAN」とは，ポート VLAN の Untagged ポートを示します。

VLAN 判定のアルゴリズムを次の図に示します。

図 7-1　VLAN 判定のアルゴリズム

7.1.5　未定義フレーム廃棄機能

未定義フレーム廃棄機能とは，予め定義した VLAN の内容と異なる条件のフレームを受信した場合に，受信フレームを廃棄する機能です。この機能を使用することによりネットワーク構成時に想定した以外の不

正アクセスのフレームを廃棄することができセキュリティを強化することが可能となります。

この機能は，適用するポートに対して「未定義フレーム廃棄機能」の対象であることを設定します。

未定義フレームの定義を次の表に示します。

表 7-5　未定義フレームの定義

フレームの種類	未定義フレームの定義
Tagged フレーム	該当ポートで明示的に tagged-port 指定していない VLAN ID を VLAN-Tag に持つフレーム
Untagged フレーム	• 該当ポートで明示的に untagged-port 指定していない場合の Untagged フレーム • プロトコル VLAN で untagged-port 指定し，かつポート VLAN の untagged-port を明示的に指定していない場合，プロトコル VLAN で指定したプロトコルと一致しないフレーム • MAC VLAN で untagged-port 指定し，かつポート VLAN の untagged-port を明示的に指定していない場合，MAC アドレスが VLAN に登録されていないフレーム

未定義フレーム廃棄機能を設定したポートは，自動的にデフォルト VLAN に加入しません。設定したポートをデフォルト VLAN に加入させるためには明示的にコンフィグレーションコマンド vlan の untagged-port サブコマンドで指定する必要があります。

7.1.6　VLAN 使用時の注意事項

(1) VLAN 数および VLAN のポート数に関する注意事項

定義する VLAN 数および VLAN 配下の Tagged ／ Untagged ポート数が多い場合，装置起動／ PSU または BSU 起動／ NIF 起動に伴う Line 起動時に Line が運用状態になるまで数十秒かかることがあります。

(2) 未定義フレーム破棄機能に関する注意事項

未定義フレーム廃棄機能は，スイッチポートだけで使用できます。ルータポートに適用することはできません。なお，ルータポートで Tag-VLAN 連携機能を使用中に未定義の VLAN Tag のフレームを受信した場合はそのフレームを廃棄します。

7.2 ポート VLAN

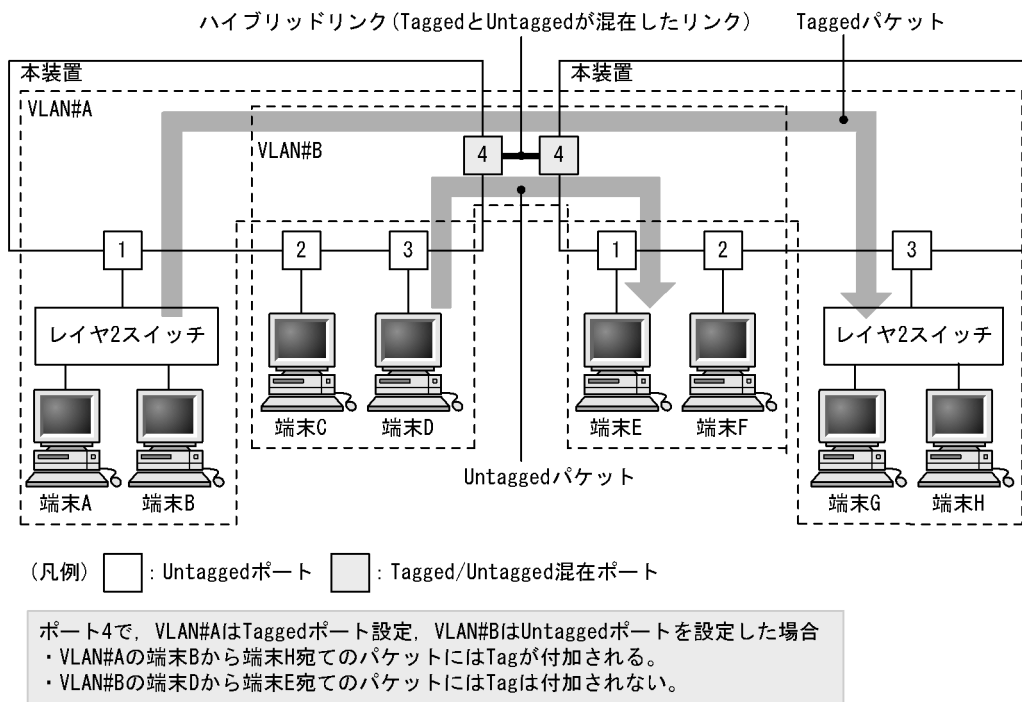
7.2.1 概要

ポート単位に VLAN のグループ分けを行います。VLAN の種類としてポート VLAN を指定し，さらに所属するポートを指定して定義します。

7.2.2 Tagged ポート /Untagged ポートの扱い

ポート VLAN では，同一ポート上で Untagged 設定と，Tagged 設定を混在できます。このように Tagged と Untagged が混在するリンクをハイブリッドリンクと呼びます。(IEEE802.1Q 規格より)

ハイブリッドリンクの構成例を次の図に示します。

図 7-2 ハイブリッドリンクの構成例

7.2.3 ポート VLAN 使用時の注意事項

(1) MAC VLAN 混在時の注意事項【SB-7800S】

同一ポートにポート VLAN と MAC VLAN が混在する場合，マルチキャスト使用時の注意事項があります。詳細は，「7.4.6 VLAN 混在時のマルチキャストについて」を参照してください。

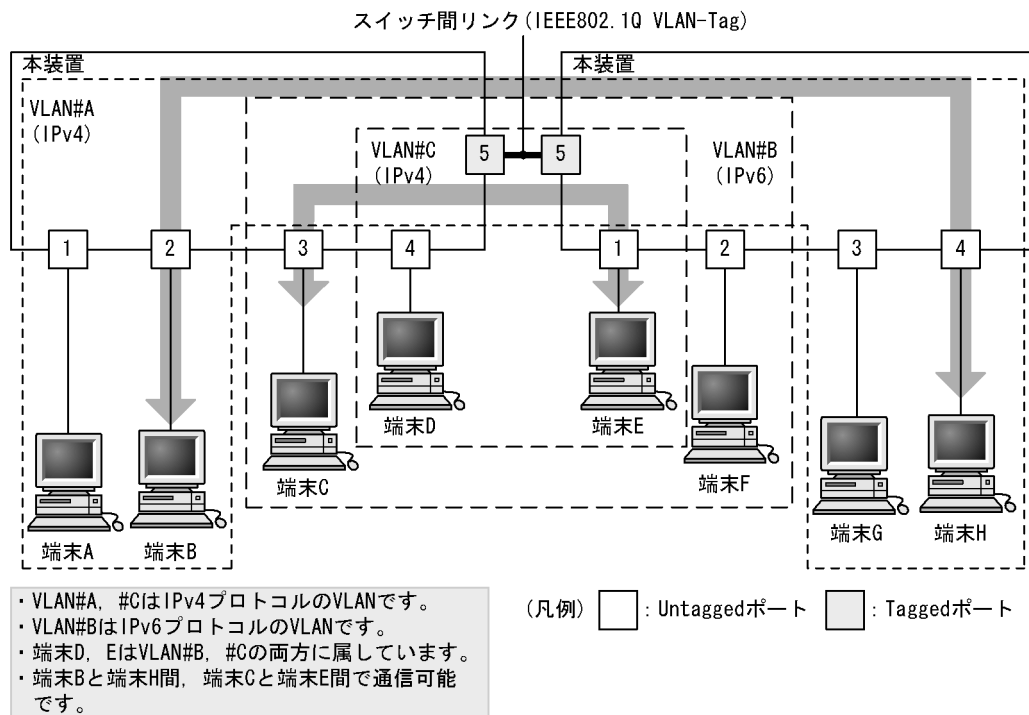
7.3 プロトコル VLAN

7.3.1 概要

プロトコル単位で VLAN のグループ分けを行います。IPv4 や IPv6 といったプロトコルごとに異なる VLAN を構成できます。複数のプロトコルを同一のプロトコル VLAN に設定することもできます。プロトコルの識別には次の 3 種類の値を使用します。

- EthernetV2 形式フレームの Ether-type 値
- 802.3 形式フレームの LLC 値 (DSAP,SSAP)
- 802.3 形式フレームの Ether-type 値

プロトコル VLAN の構成例を次の図に示します。VLAN#A，#C は IPv4 プロトコルで構成され，VLAN#B は IPv6 プロトコルで構成した例を示しています。

図 7-3　プロトコル VLAN の構成例

7.3.2 プロトコルの識別

プロトコルの識別には「7.3.1　概要」に示す 3 種類の値を使用します。

本装置では装置であらかじめ定義しているプロトコルとユーザ定義によるプロトコルを VLAN に対応付けることができます。一つのプロトコル VLAN に複数のプロトコルを対応付けることもできます。

プロトコルのうち代表的なものは，予約のプロトコル名称としてあらかじめ装置に定義されています。ユーザ定義によるプロトコルは，プロトコル名称とそれに対応するフレーム上のプロトコル値との対応を定義します。プロトコル名称とプロトコル値を次の表に示します。

表 7-6　プロトコル名称と値

プロトコル	プロトコルを識別する値	備考
IPv4	Ether-type：0x0800, 0x0806	IP，ARP
IPv6	Ether-type：0x86DD	-
ipx	Ether-type:0x8137	-
appletalk	SNAP:0x809B，0x80F3	-

（凡例）　-：該当なし

注
Ether-type：EthernetV2 形式フレームの Ether-type 値を示します
SNAP　　：802.3 形式フレームの Ether-type 値を示します

7.3.3　Tagged ポート /Untagged ポートの扱い

同一 Untagged ポート上に複数のプロトコル VLAN を設定することはできますが，同一のプロトコルのプロトコル VLAN を設定することはできません。

また，ポート VLAN の Untagged ポートとの混在もできます。ただし，混在時の受信フレームの VLAN 判定はプロトコル VLAN が優先されます。

プロトコル VLAN では，同一ポート上で Untagged 設定と Tagged 設定の混在はできません。また，MAC VLAN の Untagged ポートとの混在もできません。

7.3.4　プロトコル VLAN 使用時の注意事項

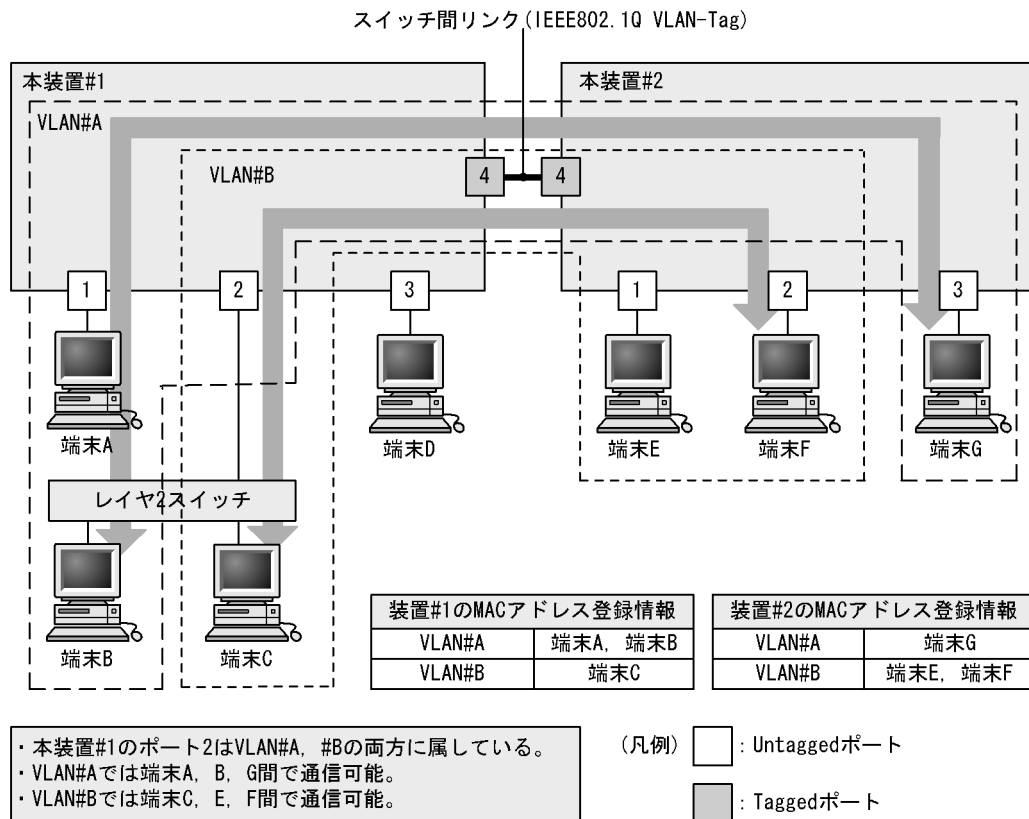
- プロトコル VLAN に IPv4 アドレスおよび IPv6 アドレスを設定することができます。ただし，IPv4 プロトコルのプロトコル VLAN に IPv6 アドレスを設定した場合など，アドレスとプロトコルが一致しない場合は設定できません。プロトコルと一致する IP アドレスを設定した場合はレイヤ 3 中継が可能となります。

7.4 MAC VLAN【SB-7800S】

7.4.1 概要

送信元の MAC アドレス単位に VLAN のグループ分けを行います。同じ MAC アドレスを複数の VLAN に設定することはできません。VLAN への MAC アドレスの登録は，コンフィグレーションによる静的な設定と，レイヤ 2 認証機能による動的な登録が可能です。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間に Tagged ポートを設定している場合は，送信元 MAC アドレスに関係なく VLAN-Tag によって VLAN を決定します。そのため，全ての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに Untagged ポートに接続した端末の MAC アドレスを設定します。

図 7-4　MAC VLAN の構成例

7.4.2 装置間の接続と MAC アドレス設定

複数の装置で MAC VLAN を構成する場合，装置間の接続は Tagged ポートを推奨します。Tagged ポートで受信したフレームの VLAN 判定は VLAN-Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。Tagged ポートで装置間を接続した場合については，「図 7-4　MAC VLAN の構成例」を参照してください。

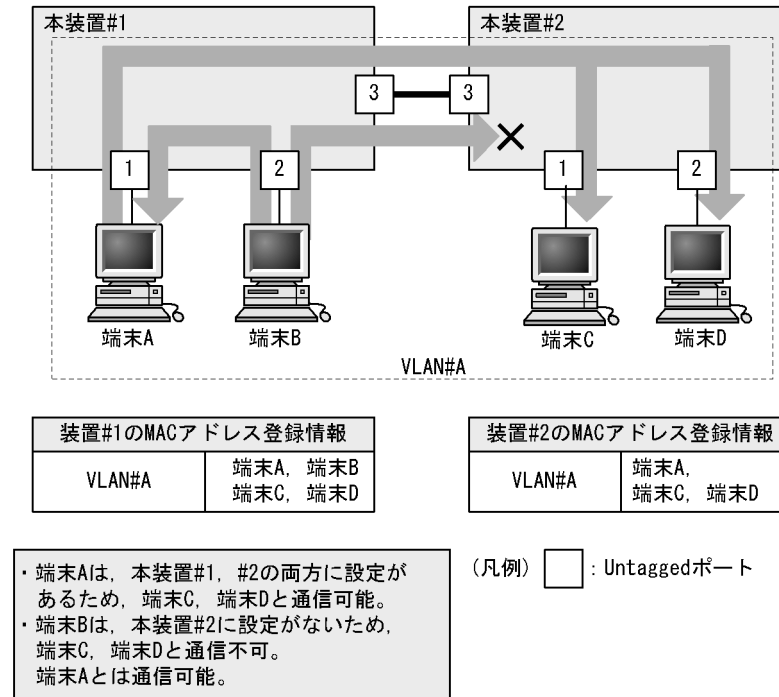
Untagged ポートで装置間を接続する場合は，その VLAN に属する全ての MAC アドレスを全ての装置に設定する必要があります。ルータが存在する場合は，ルータの MAC アドレスも登録してください。また，VRRP を使用している場合は，仮想ルータ MAC アドレスを登録してください。

Untagged ポートで装置間を接続した場合の図を次に示します。

図 7-5　装置間を Untagged ポートで接続した場合

装置#1のMACアドレス登録情報	
VLAN#A	端末A，端末B 端末C，端末D

装置#2のMACアドレス登録情報	
VLAN#A	端末A， 端末C，端末D

・端末Aは，本装置#1，#2の両方に設定が
　あるため，端末C，端末Dと通信可能。
・端末Bは，本装置#2に設定がないため，
　端末C，端末Dと通信不可。
　端末Aとは通信可能。

（凡例）□：Untaggedポート

7.4.3　Tagged ポート /Untagged ポートの扱い

MAC VLAN の Untagged ポートには，複数の MAC VLAN とポート VLAN の Untagged ポートを設定できます。Tagged ポートおよびプロトコル VLAN は設定できません。

ポート VLAN の Untagged ポートと混在している場合，受信フレームの VLAN 判定は MAC VLAN を優先します。また，Untagged ポートで受信した Tagged フレームは，ポート VLAN またはデフォルト VLAN で中継せずに廃棄します。

7.4.4　レイヤ 2 認証機能との連携について

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に設定できます。端末が接続しているポートを動的に VLAN へ設定することはできません。

レイヤ 2 認証機能を次に示します。

- IEEE802.1X 機能

プリンタやサーバなど，レイヤ 2 認証機能が動作せずに Untagged ポートと接続する端末は，その MAC アドレスをコンフィグレーションで VLAN に設定します。

コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの設定が有効になります。

7.4.5　MAC VLAN サポートの PSU について

MAC VLAN の Tagged ポートは，全ての PSU で動作します。Untagged ポートは PSU-43 だけで動作し，それ以外の PSU では動作しません。PSU-43 以外に実装されているポートに Untagged ポートを設定した場合，該当するポートではリンクアップのまま通信をすべて遮断します。ただし，レイヤ 2 プロトコルの制御フレームは正常に送受信するため，LACP やスパニングツリーなどは動作します。

リンクアグリゲーション内のポートの場合は，リンクアグリゲーション全体ではなく，該当するポートだけ通信を遮断します。

表 7-7　MAC VLAN サポート PSU

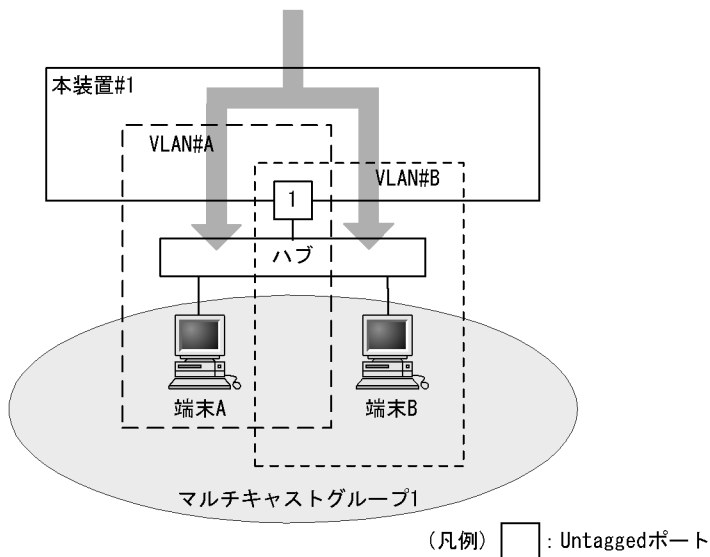
種別	PSU-43	PSU-43 以外	備考
Untagged ポート	○	×	PSU-43 以外では通信を遮断
Tagged ポート	○	○	なし

（凡例）○：動作可　　×：動作不可

7.4.6　VLAN 混在時のマルチキャストについて

同一ポートに複数の MAC VLAN を混在した場合やポート VLAN と MAC VLAN を混在した場合，それぞれの VLAN に所属する端末が同じマルチキャストグループに所属すると，そのポートへは VLAN ごとに同じマルチキャストフレームを送信するため，端末は同じフレームを重複して受信します。

端末でマルチキャストデータを重複して受信してしまうネットワークの構成例を次に示します。

図 7-6　VLAN 混在時のマルチキャスト

7.5 VLAN 拡張機能

7.5.1 アップリンク VLAN

（1） 概要

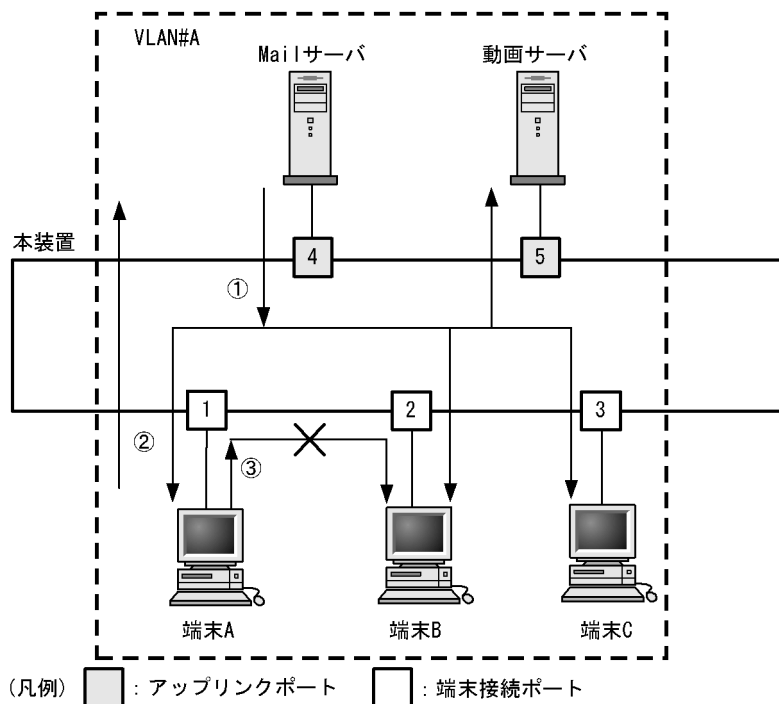
アップリンク VLAN 機能とは，VLAN 内で，端末を接続するポート（端末接続ポート）間での通信（レイヤ 2 中継）を遮断する機能です。通信を遮断する端末接続ポートと，そうでないポート（アップリンクポート）を明示的に定義します。

アップリンクポート間，およびアップリンクポートと端末接続ポート間でだけ通信を行い，端末接続ポート間ではフレームの中継を行いません。端末同士の直接通信を遮断して，セキュリティを確保したい場合などに適用できます。適用例を次の図に示します。

この適用例は，VLAN 内でアップリンクポートには共用サーバなどを接続し，端末接続ポートには端末を接続します。これによって，端末間での通信を遮断し端末と共用サーバ間でだけ通信を可能にします。

図 7-7　アップリンク VLAN の適用例

VLAN#A
Mailサーバ
動画サーバ
本装置
4
5
①
1
2
3
②
③
端末A
端末B
端末C

（凡例）：アップリンクポート　：端末接続ポート

①アップリンクポートからのブロードキャストパケットは全ポートへ中継
②アップリンクポート-端末接続ポート間での中継は可能
③端末接続ポート間の中継は遮断

（2） アップリンク VLAN 機能のモード

アップリンク VLAN は loose モードと strict モードの二つのモードがあります。

- loose モード
  端末接続ポート間で，ブロードキャスト，マルチキャスト，未学習のユニキャストの中継を遮断します。学習済みのユニキャストは遮断せず中継します。
- strict モード

端末接続ポート間で，すべての通信を遮断します。loose モードで中継するユニキャストについてもすべて遮断します。

(3) アップリンク VLAN 機能使用時の注意事項

(a) FDB エントリ消費量について

アップリンク VLAN 機能では，MAC 学習で一つの MAC アドレスにつき複数の FDB エントリを消費するケースがあります。詳細は「6.2.6　注意事項 (1) MAC アドレス学習の FDB 消費量」を参照してください。

(b) スパニングツリーを同時に使用するときの注意事項

端末接続ポートでスパニングツリーを運用するとトポロジーによって通信不可となる場合があります。

7.5.2　アップリンクブロック

(1) 概要

アップリンクブロック機能は，VLAN 内のポートを「冗長構成を接続するアップリンク」と「その他の端末接続ポート」に分け，冗長構成を接続するアップリンク間での中継を抑止する機能です。

本装置が冗長構成の下流に接続している場合に，ネットワーク構築中の一時的なループや冗長プロトコルの不具合によるループが発生した場合にフレームループを回避したい場合に適用できます。

アップリンク VLAN 機能が端末接続ポート間の中継を抑止するのに対し，アップリンクブロック機能はアップリンク間の中継を抑止します。適用例を次の図に示します。

この適用例は，GSRP 機能と合わせて使用する例を示します。GSRPaware で上位の GSRP スイッチ間のレイヤ 2 中継を抑止することによってループ回避を実現します。

図 7-8 アップリンクブロックの適用例

(2) アップリンクブロック機能使用時の注意事項

(a) FDB エントリ消費量について

アップリンクブロック機能では，MAC 学習で一つの MAC アドレスにつき複数の FDB エントリを消費するケースがあります。詳細は「6.2.6　注意事項　(1) MAC アドレス学習の FDB 消費量」を参照してください。

7.5.3 プライベート VLAN

(1) 概要

プライベート VLAN 機能とは，複数の VLAN を組み合わせて一つのサブネットを構成する機能です。プライベート VLAN を構成する各 VLAN には，用途に応じて Primary VLAN，Secondary VLAN(isolated VLAN)，Secondary VLAN(community VLAN) のどれかの VLAN タイプを定義します。

各 VLAN タイプについて以下に説明します。

- Primary VLAN
  Primary VLAN は一つのサブネットを構成する複数の VLAN を束ねるための VLAN です。Primary VLAN には複数の Secondary VLAN を対応付けることができます。Primary VLAN 側で受信したフレームは，Primary VLAN 内のすべてのポートと，Primary VLAN に対応付けられているすべての Secondary VLAN のポートに中継することができます。

複数の Secondary VLAN から共有して使用する装置がある場合にはこの VLAN に収容します。
Primary VLAN には IP アドレスを設定することができます。IP アドレスを設定することで，Secondary VLAN から受信したパケットについても L3 中継が可能となります。

- Secondary VLAN
  一つの Secondary VLAN に対して一つの Primary VLAN を対応付けることができます。一つの Secondary VLAN が複数の Primary VLAN と対応関係を持つことはできません。Secondary VLAN には isolated VLAN と community VLAN の二つのタイプがあります。
  1. isolated VLAN
     isolated VLAN 側で受信したフレームを同一 VLAN 内のポートへは中継せずに，対応付けられている Primary VLAN のポートへだけ中継することができます。したがって，isolated VLAN 側のポートに接続されている端末は端末同士の通信ができなくなり，代わりに Primary VLAN 側に接続されている装置との通信だけができるようになります。端末間の通信を遮断し，セキュリティを向上させたいときに使用します。
     一つの Primary VLAN に対応付けることができる isolated VLAN は，最大で一つです。
  2. community VLAN
     community VLAN 側で受信したフレームを同一 VLAN 内のポートと，Primary VLAN のポートの両方へ中継することができます。したがって，community VLAN 側のポートに接続されている端末は community VLAN 単位にグループ化され，さらに Primary VLAN 側に接続されている装置との通信も可能となります。教室や会議室といった単位で端末をグループ化し，グループ間での通信を遮断しつつグループ内の端末間の通信を許可する場合に使用します。

  Secondary VLAN には IP アドレスを設定できません。

Primary VLAN で受信したフレームを中継することができるポートの範囲と，Secondary VLAN で受信したフレームを転送することができるポートの範囲を，次の図に示します。

図 7-9　Primary VLAN で受信した場合の中継可能なポートの範囲

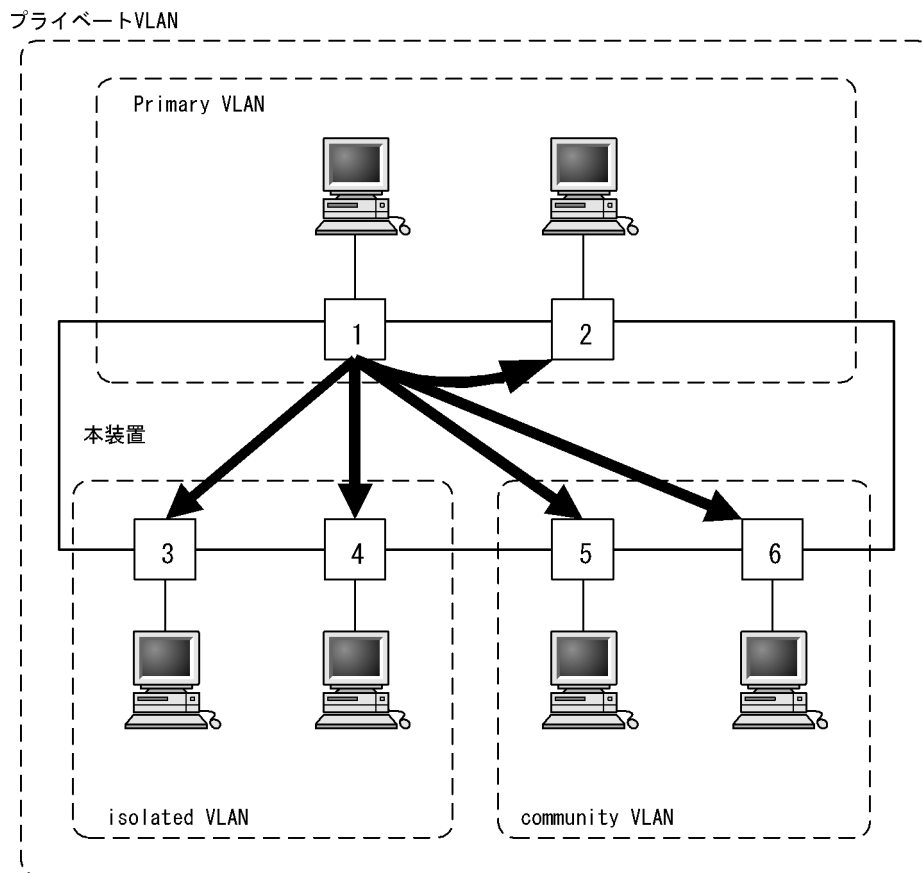
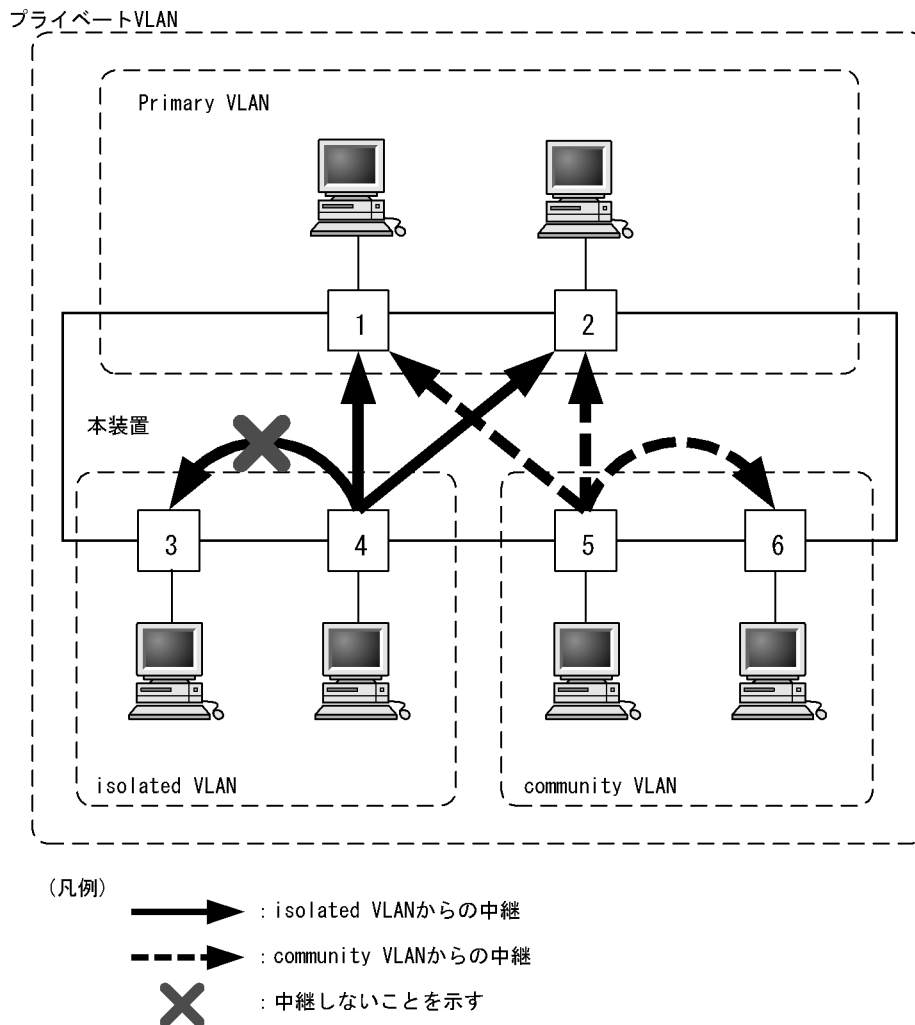
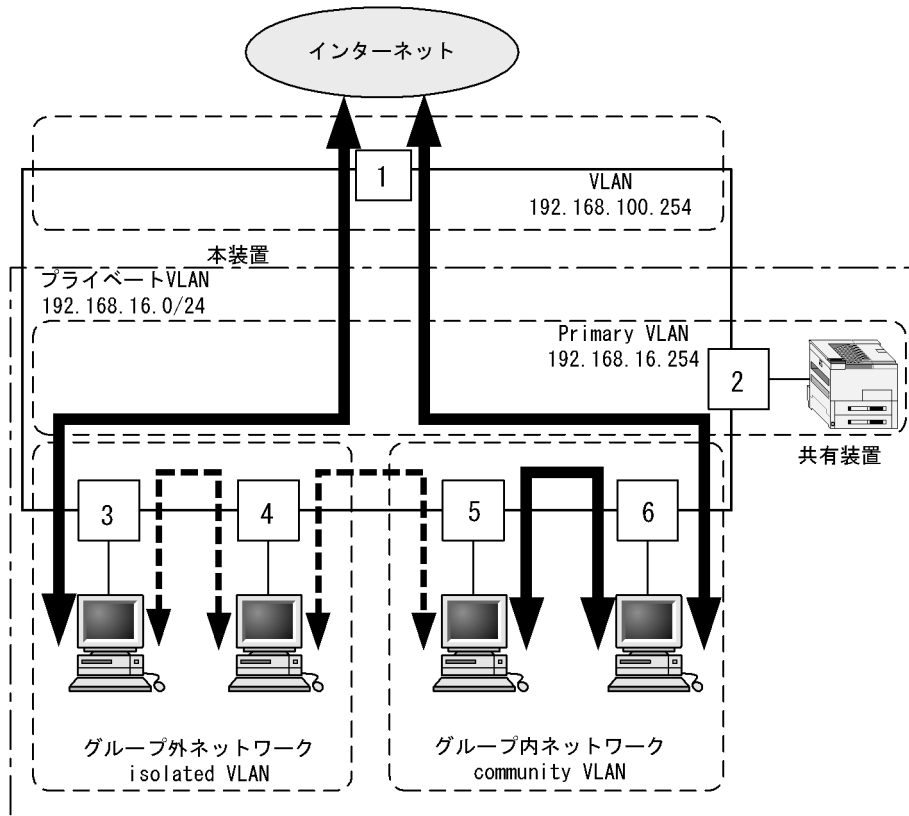
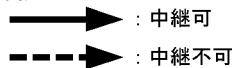



図 7-10　Secondary VLAN で受信した場合の中継可能なポートの範囲

以下にプライベート VLAN 機能の適用例を示します。

この適用例は，ある一つのサブネットを信頼できる端末の所属するネットワーク (グループ内ネットワーク) と，信頼できない端末の所属するネットワーク (グループ外ネットワーク) に分けた場合を示しています。信頼できない端末を接続するネットワークについては，端末間の通信を遮断して端末間のセキュリティを確保することができます。また，信頼できる端末のネットワークについては，端末間の通信を許可しています。双方のネットワークから共有する必要のあるプリンタなどの装置については Primary VLAN 側に接続します。

Primary VLAN に IP アドレスを設定することで，Primary VLAN がこのサブネットのルータとして動作し，Secondary VLAN からのデータをルーティングすることが可能です。

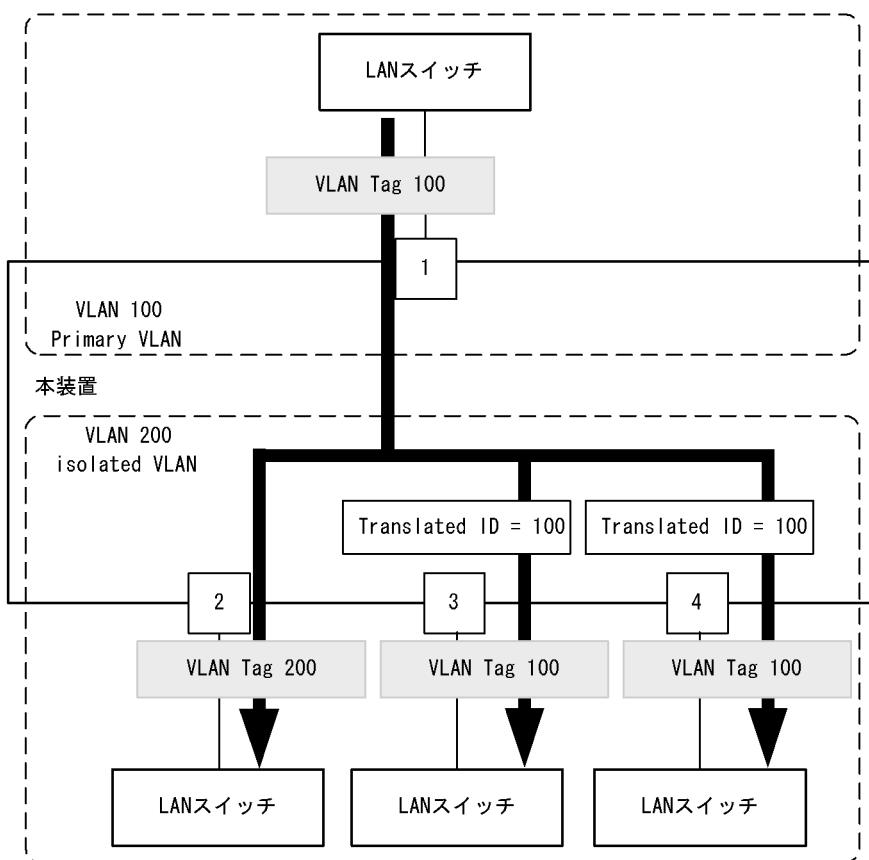
図 7-11　プライベート VLAN の適用例

（2） プライベート VLAN 機能使用時の注意事項

（a）FDB エントリ消費量について

プライベート VLAN 機能では，MAC 学習時に一つの MAC アドレスにつき複数の FDB エントリを消費するケースがあります。詳細は「6.2.6　注意事項　（1）MAC アドレス学習の FDB 消費量」を参照してください。

（b） プライベート VLAN の Tagged ポートについて

プライベート VLAN に所属する Tagged ポートでは，プライベート VLAN の各 VLAN の VLAN-Tag で送受信を行います。Primary VLAN と Secondary VLAN で同じ VLAN-Tag を使用する場合は，Tag 変換機能を設定してください。

図 7-12　Tag 変換機能を使用したプライベート VLAN

(c) フィルタリングおよび QoS 機能について

プライベート VLAN 機能を使用している VLAN に対するフィルタリング，および QoS 機能は，該当 VLAN の物理ポート (<Portlist> 指定) に対する設定だけサポートしています。該当 VLAN のインタフェース (<Interface Name> 指定) に対する設定は未サポートです。

(d) プライベート VLAN の設定について

プライベート VLAN の設定時には，次に示す項目に注意してください。

- 一つの VLAN には，Primary VLAN または Secondary VLAN のどちらか一方だけ設定できます。
- 複数の Primary VLAN から同一の Secondary VLAN を対応づけることはできません。
- Primary VLAN から Primary VLAN を対応づけに指定できません。
- 対応関係を設定する VLAN で，FDB のスタティックエントリに同じ MAC アドレスは指定できません。

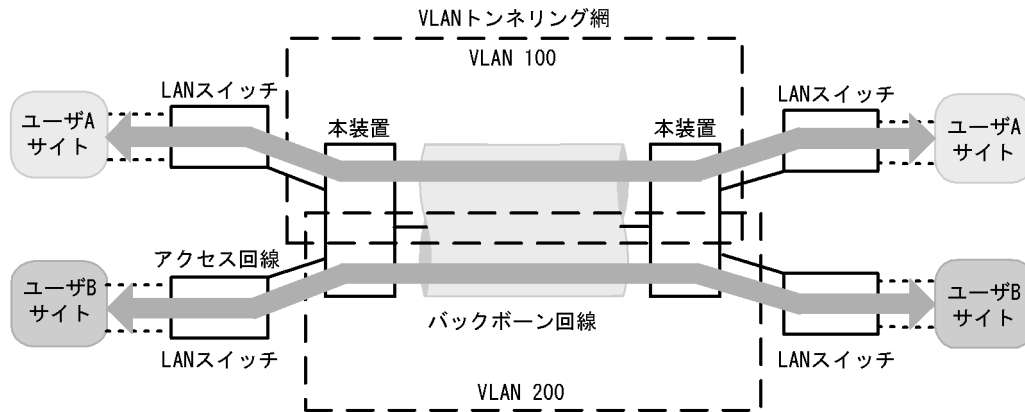
7.5.4　VLAN トンネリング

(1) 概要

VLAN トンネリング機能とは，複数ユーザの VLAN をほかの VLAN の中に集約して「トンネル」する機能です。IEEE802.1Q VLAN-Tag をスタックすることで一つの VLAN 内にほかの VLAN に属するフレームをトランスペアレントに通すことができます。トンネルは 3 個所以上のサイトを接続するマルチポイント接続が可能です。適用例を次の図に示します。

この適用例では，レイヤ 2 VPN サービスである広域イーサネットサービスに適用する場合を例に示しま

す。本装置に VLAN トンネリング機能を適用します。本装置で VLAN-Tag をスタックして図中の LAN スイッチ間の通信をトランスペアレントに行うことができます。

図 7-13　VLAN トンネリング概要（広域イーサネットサービス適用例）

(2) VLAN トンネリング機能を使用するための必須条件

VLAN トンネリング機能を使用する場合は，下記の設定が必須となります。

- コンフィグレーションコマンド vlan-tunneling-enable を設定する。
- VLAN トンネリング機能を実現する VLAN では，アクセス回線側は Untagged ポートを定義，バックボーン回線側は Tagged ポートを定義する（アクセス回線側とバックボーン回線側を同じポートで共用することはできない）。
- VLAN トンネリングのバックボーン回線はコンフィグレーションコマンド line の jumbo-frame サブコマンドもしくは ethernet-jumbo-frame コマンドで，1,522 バイト以上（FCS を除く）を設定する。

(3) VLAN トンネリング機能使用時の注意事項

(a) デフォルト VLAN について

デフォルト VLAN の自動加入を行いません。すべての VLAN を明示的に設定してください。

(b) スパニングツリーについて

Untagged ポート（アクセス回線側）ではスパニングツリーは動作しません。Tagged ポート（バックボーン回線側）だけでスパニングツリーを使用できます。

(c) VLAN Tag スタックの段数について

VLAN Tag のスタックは 2 段のスタックをサポートします。3 段以上スタックしているフレームを扱うことはできません。

(d) レイヤ 3 インタフェースの使用について

VLAN トンネリング機能使用時は，VLAN に IP アドレスを設定することはできません。本装置の管理などを目的とした IP アドレスは，次に示すどれかを使用してください。

- RM イーサネットインタフェース**【SB-7800S】**
- リモートマネージメントポートもしくはメンテナンスポート**【SB-5400S】**
- ルータポート

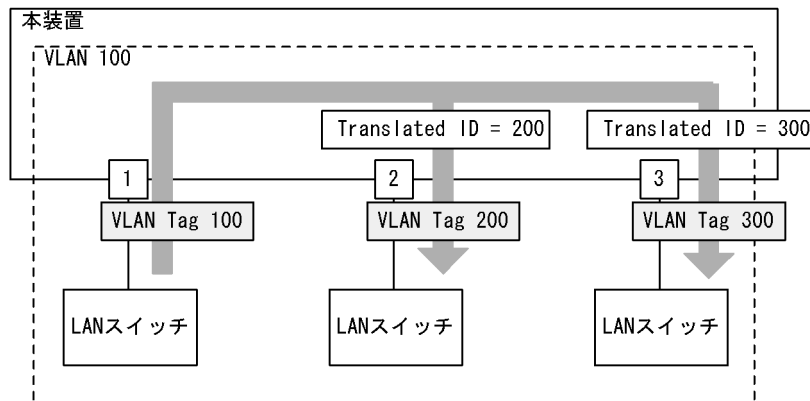
7.5.5 Tag 変換機能

(1) 概要

Tag 変換機能は，Tagged フレームをレイヤ 2 スイッチ中継する際に，フレームの VLAN Tag の VLAN ID フィールドを別の値に変換する機能です。この機能によって，異なる VLAN ID で設定した既設の VLAN を一つの VLAN として接続することが可能となります。

Tag 変換機能は，VLAN の Tagged ポートでポートごとに指定します。Tag 変換機能を使用しない通常の Tagged ポートでは，VLAN Tag の VLAN ID フィールドにコンフィグレーションで指定した VLAN の VLAN ID を使用します。Tag 変換機能を指定した場合はその ID を使用します。その ID のことを Translated ID と呼びます。

Tag 変換機能の構成例を次の図に示します。図では，ポート 1 は Tag 変換機能未指定であり，ポート 2 およびポート 3 にそれぞれ Tag 変換機能を設定し，VLAN Tag の VLAN ID フィールドを変換して中継します。

図 7-14 Tag 変換機能の構成例

(2) Tag 変換機能使用時の注意事項

Tag 変換機能を設定したポートで未定義フレーム廃棄機能を使用した場合，未定義フレームの判定を Translated ID で行うため注意してください。

7.5.6 L2 プロトコルフレーム透過機能

(1) BPDU フォワーディング機能

(a) 概要

この機能は，スパニングツリーを使用しない VLAN で BPDU を中継する機能です。通常 BPDU は VLAN 内では中継しません。

中継する BPDU は本装置から見ると単なるマルチキャストフレームとなり，スパニングツリーの計算には使用しません。

VLAN トンネリングでこの機能を使用すると，ユーザの BPDU を通過させることができます。その際，すべてのエッジ装置，コア装置で BPDU フォワーディング機能を設定する必要があります。

(b) BPDU フォワーディング機能使用時の注意事項

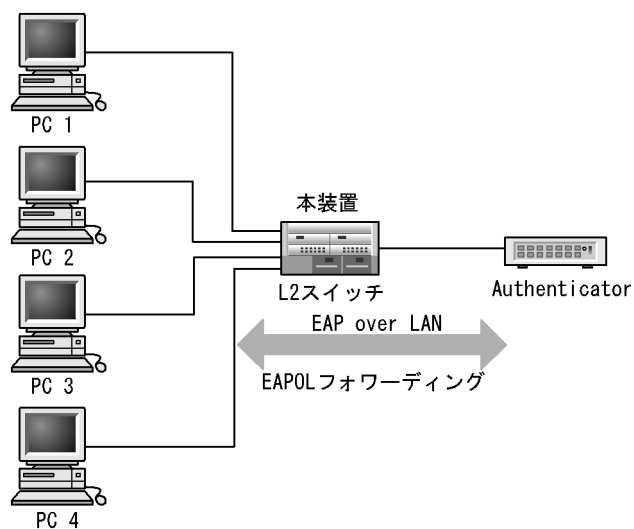
ポート VLAN の untagged-port を指定している VLAN で適用すると，シングルスパニングツリーおよびマルチプルスパニングツリーの BPDU を中継します。

(2) EAPOL フォワーディング機能

(a) 概要

この機能は，IEEE 802.1X を使用しない VLAN で EAPOL を中継する機能です。通常 EAPOL は VLAN 内では中継しません。

中継する EAPOL は本装置から見ると単なるマルチキャストフレームとなり，IEEE 802.1X の認証には使用しません。

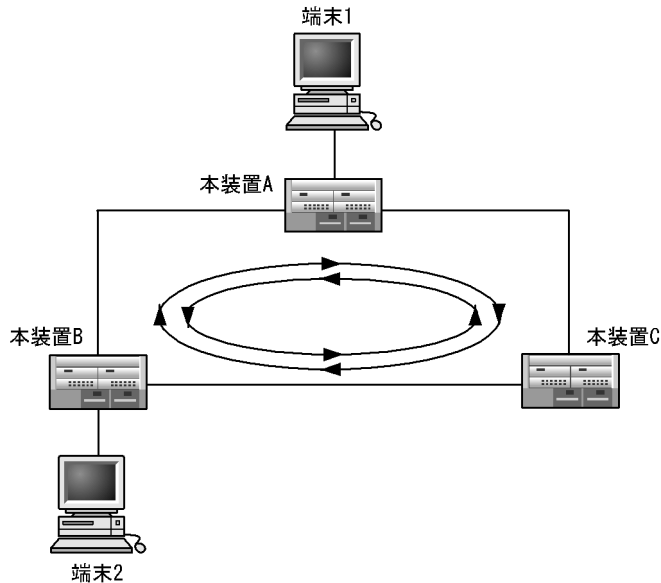
本装置を，Authenticator と端末 (Supplicant) の間の L2 スイッチとして用いるときにこの機能を使用します。

スパニングツリー

スパニングツリーはスイッチ間のループ防止機能です。この章ではスパニングツリーについて説明します。

8.1　スパニングツリー概説

8.1.1　概要

スパニングツリープロトコルは，ループ防止プロトコルです。スパニングツリープロトコルを使用することで，スイッチ間でお互いに通信し，ネットワーク上の物理ループを発見することができます。スイッチ接続のネットワーク上のループが発生した場合の問題点について次の図に示します。

図 8-1　ネットワーク上でのループ発生時の問題点

端末 1 が端末 2 に対してフレームを最初に送信した場合を例とします。

- 端末 1 によって端末 2 に送信されたフレームは，本装置 A によって受信されます。これが，端末 1 と端末 2 の間でやり取りされる最初のフレームであるため，本装置 A，B，C の FDB には端末 1 に対するエントリの登録はまだ行われていません。
- 本装置 A は端末 1 の MAC アドレスとポートとのマッピングを FDB に登録しフレームをフラッディングします。本装置 A によりフラッディングしたフレームを本装置 B および本装置 C が受け取ると，それぞれが端末 1 から最初に受けたフレームのため，端末 1 の MAC アドレスと本装置 A 側ポートとのマッピングを FDB に登録しフレームをフラッディングします。
- それにより本装置 B は本装置 C からフラッディングされた端末 1 からの送信フレームを受信したときに，最初のエントリを削除し端末 1 の MAC アドレスを本装置 C 側ポートにマッピングするエントリを FDB に登録します。同様に本装置 C は本装置 B よりフラッディングされたフレームを受信したときに最初のエントリを削除し端末 1 の MAC アドレスを本装置 B 側ポートにマッピングするエントリを FDB に登録します。
- この結果，全装置とも端末 1 の MAC アドレスが複数のポート間で交互に切り替り登録され，FDB が不安定な状態となり，どの装置もフレームを端末 1 に正しく転送できなくなってしまいます。

スパニングツリープロトコルは，このようなループを防止することを目的としています。

8.1.2　スパニングツリーの種類

本装置では，シングルスパニングツリー，PVST+，およびマルチプルスパニングツリーの 3 種類のスパニ

ングツリーをサポートします。各スパニングツリーは構築の単位が異なります。スパニングツリーの種類と概要について次の表に示します。

表 8-1　スパニングツリーの種類

名称	構築単位	概要
シングルスパニングツリー	装置単位	装置全体のポートを対象としツリーを構築します。VLAN 構成とは無関係に構築するため，一つのポートに複数の VLAN が所属している場合では，すべての VLAN に同じツリー構築結果を適用します。
PVST+	VLAN 単位	VLAN 単位にツリーを構築します。一つのポートに複数の VLAN が所属している場合，VLAN ごとに異なるツリー構築結果を適用します。
マルチプルスパニングツリー	MST インスタンス単位	複数の VLAN をまとめた MST インスタンスというグループごとにスパニングツリーを構築します。一つのポートに複数の VLAN が所属している場合，MST インスタンス単位に異なるツリー構築結果を適用します。

本装置では，上記で記述したスパニングツリーを単独あるいは組み合わせて使用することができます。スパニングツリーの組み合わせと適用範囲を次の表に示します。

表 8-2　スパニングツリーの組み合わせと適用範囲

ツリー構築条件	トポロジー計算結果の適用範囲
シングルスパニングツリー単独	全 VLAN にシングルスパニングツリーを適用します。
PVST+ 単独	PVST+ を設定している VLAN には VLAN ごとのスパニングツリーを適用します。その他の VLAN はスパニングツリーを適用しません。
シングルスパニングツリーと PVST+ の組み合わせ	PVST+ を設定している VLAN には VLAN ごとのスパニングツリーを適用します。その他の VLAN にはシングルスパニングツリーを適用します。untagged-port 設定したポートでは，シングルスパニングツリーが Disable 状態になる場合があります。「8.3　PVST+」を参照してください。
マルチプルスパニングツリー単独	全 VLAN にマルチプルスパニングツリーを適用します。

注　マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

8.1.3　スパニングツリートポロジーの構成要素

スパニングツリーを構築するために使用するブリッジやポートの役割，およびそれらの役割を決定するために用いる識別子について以下に示します。

(1)　ルートブリッジ・指定ブリッジ

- ルートブリッジ
  ツリーを構築しているスイッチ内の論理的な中心となるスイッチでツリー内に一つだけルートブリッジはあります。
- 指定ブリッジ
  ルートブリッジの方向から特定のリンクへ向かうトラフィックの転送を担当するスイッチは，そのリンクの指定ブリッジと呼びます。

(2)　ルートポート・指定ポート

ツリー内の指定ブリッジは，以下の 3 種類のポートを持ちます。ルートブリッジはすべてのポートが指定ポートとなります。

- ルートポート
  指定ブリッジからルートブリッジに向かう接続性を提供するポートで，「通信可」状態のポートです。
- 指定ポート
  ルートブリッジ，または指定ブリッジから各リンクへ向かう方向のポートで「通信可」状態のポートです。
- 非指定ポート
  ルートポート・指定ポート以外のポートで，「通信不可」状態のポートです。
  冗長構成時にルートポート上に障害が発生した場合にはルートポートになる可能性のあるポートや，故障時や管理上の制御によって「転送不可」状態になっているポートを含みます。

(3) ブリッジ識別子・ポート識別子

- ブリッジ識別子
  ネットワーク内の個々のスイッチに一意な識別子です。ブリッジ識別子はブリッジ優先度（16bit）とブリッジ MAC アドレス（48bit）で構成されます。ブリッジ優先度の下位 12bit は拡張システム ID です。拡張システム ID には，シングルスパニングツリー，マルチプルスパニングツリーの場合は 0 が設定され，PVST+ の場合は VLAN ID が設定されます。ブリッジ識別子を次の図に示します。

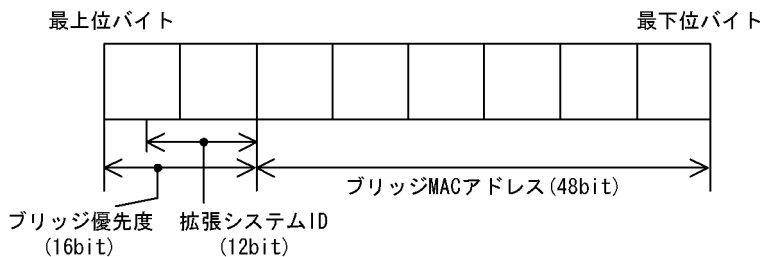
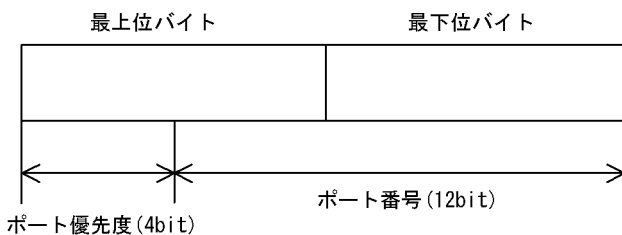
図 8-2　ブリッジ識別子

- ポート識別子
  スイッチ内の各ポートを一意に識別するために割り当てる識別子です。ポート識別子はポート優先度（4bit）とポート番号（12bit）によって構成されます。ポート識別子を次の図に示します。

図 8-3　ポート識別子

(4) パスコスト・ルートパスコスト

- パスコスト
  スイッチ上の各ポートのデータレートに対応するコスト値を示します。イーサネット回線の速度が速いほどコスト値は低くすることを推奨しています。パスコストはコンフィグレーションにより設定することが可能です。
  リンクアグリゲーショングループのパスコストは集約しているポート本数に関わらず，ポート 1 本分のパスコスト値となります。リンクアグリゲーショングループを優先して使用したい場合は，パスコスト値を低くしてください。
- ルートパスコスト
  ルートパスコストはルートブリッジに至るすべてのポートのパスコストが累積された値です。スパニン

グツリーでは最もコストの低いパスで接続する構成でツリーを構築します。

8.1.4　スパニングツリーの構築

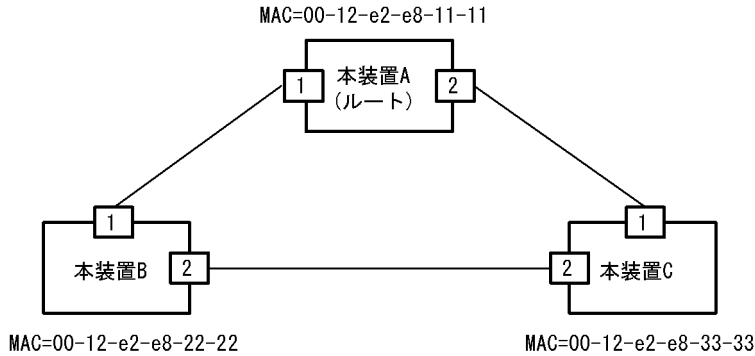
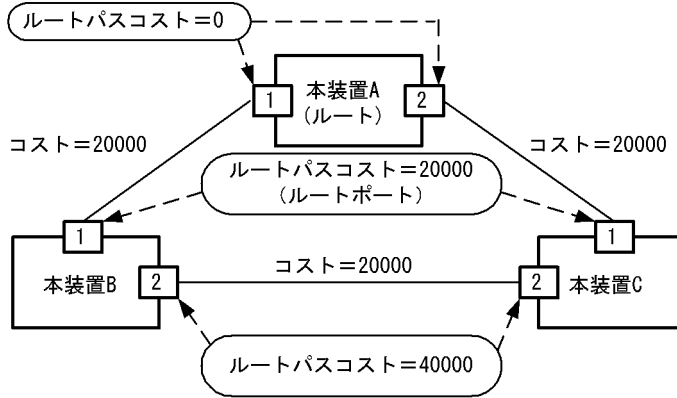
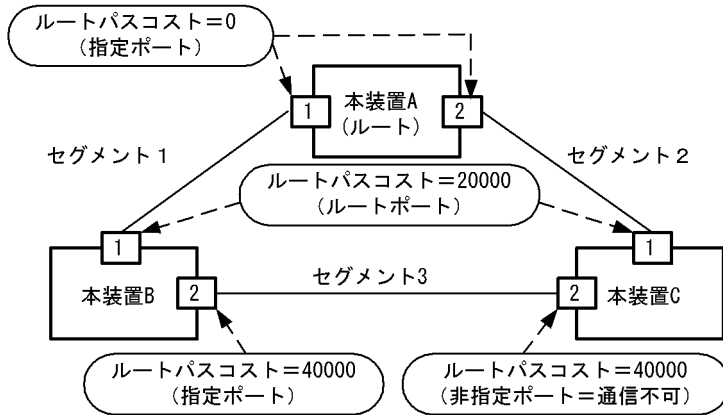
スパニングツリートポロジーは，ブリッジ識別子，パスコスト，およびポート識別子を以下の優先度に従ってトポロジーを構築します。

1. 最小ルートブリッジ識別子
2. 最小ルートパスコスト
3. 最小送信元ブリッジ識別子
4. 最小送信元ポート ID

ネットワーク内のスイッチ同士は BPDU(Bridge Protocol Data Unit) のフレームを使ってこれらの情報を含むスパニングツリー情報を交換します。スパニングツリーを構築するまでを以下の 3 段階に分けることができます。

1. ルートブリッジの選出
   ネットワーク内で最小のブリッジ識別子を持つスイッチがルートブリッジになります。「図 8-4　スパニングツリーの構築」の (1) の例の場合はブリッジ優先度を全装置ともデフォルト値としているため最小の MAC アドレスを持つ本装置 A がルートブリッジとなります。
2. ルートポートの選出
   ルートブリッジの選出が完了するとルートポートの選出を行います。ルートポートの選出にはルートパスコスト値が最も小さいポートを選出します。「図 8-4　スパニングツリーの構築」の (2) の例の場合，本装置 B，C のポート 1 がそれぞれの装置内で最小のルートパスコストを持つためルートポートになります。
3. 指定ポートの選出
   ネットワーク上の一つのセグメントには一つの指定ポートを選出します。この指定ポートが自分のセグメントとルートブリッジの間でトラフィックの送信を行う唯一のポートとして機能することでループを回避することができます。指定ポートの選出もルートパスコスト値が最も小さいポートを選出します。「図 8-4　スパニングツリーの構築」の (3) の例の場合，ルートブリッジである本装置 A と接続しているセグメント 1，2 については本装置 A がルートブリッジであるため全ポートが指定ポートとなります。セグメント 3 については，本装置 B のポート 2 と本装置 C のポート 2 のルートパスコストが同一値となり，二つのポートは対等となります。これによって次の判断基準である送信元ブリッジ識別子で比較することになります。本装置 B の方が本装置 C よりブリッジ識別子は小さいため本装置 B のポート 2 がセグメント 3 の指定ポートになり，本装置 C のポート 2 は非指定ポートとなり「通信不可」状態のポートとなることでループを回避しスパニングツリーの構築が完了します。

図 8-4　スパニングツリーの構築

(1)ルートブリッジの選出
ブリッジ優先度は全装置デフォルト値を使用している場合，MACアドレスの最も小さい本装置Aがルートブリッジとなる。

(2)ルートポートの選出
本装置B内のポート1，2では最小のルートパスコストを持つポート1がルートポートとなる。
本装置Cも同様にポート1がルートポートとなる。

(3)指定ポートの選出
本装置A内のポート1，2，本装置Bのポート2が指定ポート。
本装置Cのポート2が非指定ポートとなり通信不可状態となることでループを回避しツリー構築が完了。

8.1.5　STP 互換モード

(1)　概要

シングルスパニングツリーの RSTP，PVST+ の RSTP，およびマルチプルスパニングツリーで，対向装置

がシングルスパニングツリーの STP または PVST+ の STP の場合，該当するポートは STP 互換モードで動作します。STP 互換モードで動作すると，該当するポートで高速遷移が行われなくなり，通信復旧に時間が掛かるようになります。対向装置がシングルスパニングツリーの RSTP，PVST+ の RSTP，およびマルチプルスパニングツリーに変わった場合，STP 互換モードから復旧し，再び高速遷移が行われるようになりますが，タイミングによって該当するポートと対向装置が STP 互換モードで動作し続ける場合があります。STP 互換モード復旧機能は，STP 互換モードで動作しているポートを強制的に復旧させ，高速遷移が正常に行えるようにします。

(2) 復旧機能

運用コマンド clear spanning-tree detected-protocol を実行することによって，STP 互換モードから強制的に復旧します。該当するポートのリンクタイプが point-to-point，shared のどちらの場合でも動作します。

(3) 自動復旧機能

該当するポートのリンクタイプが point-to-point の場合，STP 互換モード復旧機能が自動で動作します。該当するポートが非指定ポートで STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することによって，STP 互換モードを解除します。

該当するポートのリンクタイプが shared の場合（複数の装置が接続される場合），自動復旧モードが正しく動作できないため，自動復旧モードは動作しません。

8.2 シングルスパニングツリー

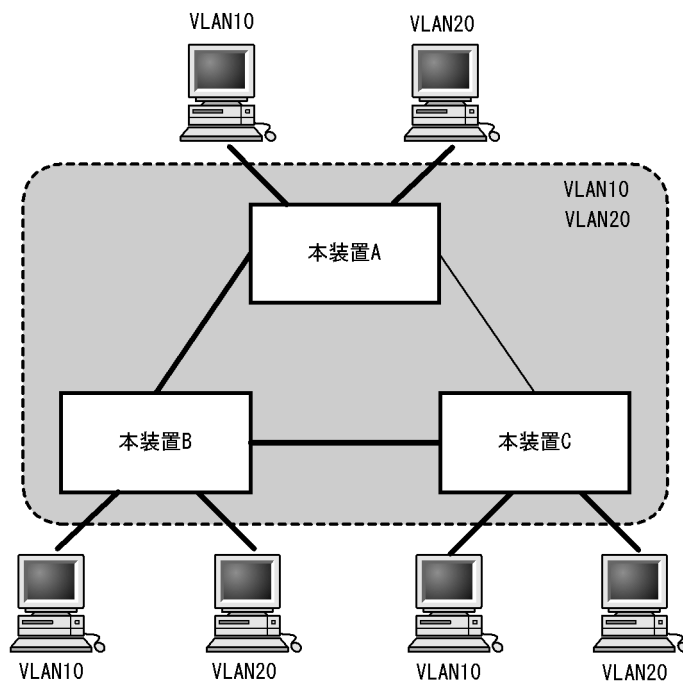
シングルスパニングツリーは装置全体のスイッチポートを対象としツリーを構築します。

8.2.1 適用するネットワーク構成

シングルスパニングツリーでは，一つのスパニングツリーですべての VLAN のループを回避できます。VLAN ごとに制御する PVST+ よりも多くの VLAN を扱うことができます。

シングルスパニングツリーによるネットワーク構成を次の図に示します。

この図では，本装置 A，B，C に対して，VLAN 10 および VLAN 20 を設定し，これらの VLAN で一つのトポロジーを使用して通信しています。

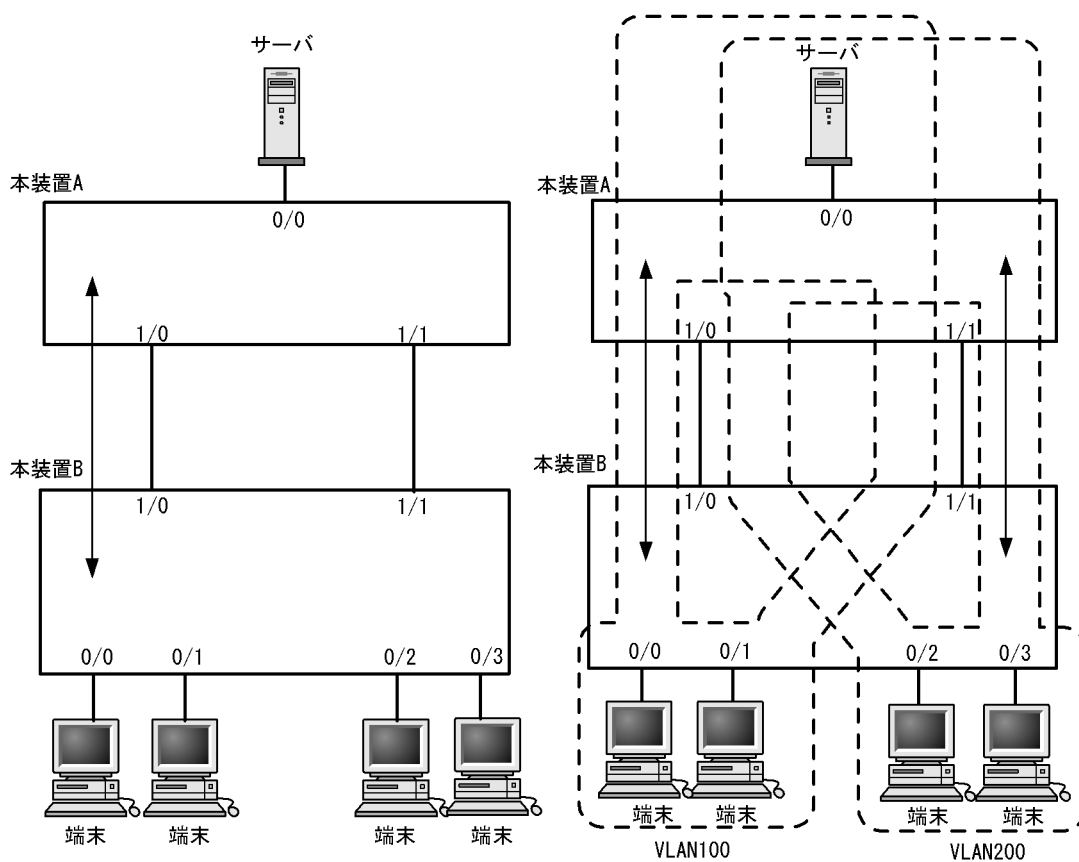
図 8-5　シングルスパニングツリーによるネットワーク構成

8.3　PVST+

PVST+ は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，ポート VLAN の untagged-port では，シングルスパニングツリーで動作しているスイッチと接続することが可能です。

8.3.1　PVST+ によるロードバランシング

次の図に示すような本装置 A，B 間を冗長パスを組んだネットワークにおいてシングルシングルスパニングツリーを組んだ場合，各端末からサーバへのアクセスは当然ながら本装置 A，B 間のポート 1 に集中します。そこで，複数の VLAN を組み PVST+ により VLAN ごとに別々のトポロジーとなるように設定することで冗長パスとして使用可能となり，さらに負荷分散を図ることが可能となります。ポート優先度によるロードバランシングの例を次の図に示します。

この例では，VLAN100 に対してはポート 1/0 のポート優先度をポート 1/1 より高く設定し，逆に VLAN200 に対しては 1/1 のポート優先度をポート 1/0 より高く設定することで，各端末からサーバに対するアクセスを VLAN ごとに負荷分散を行っています。

図 8-6　PVST+ によるロードバランシング

8.3.2　シングルスパニングツリーとの接続ポート

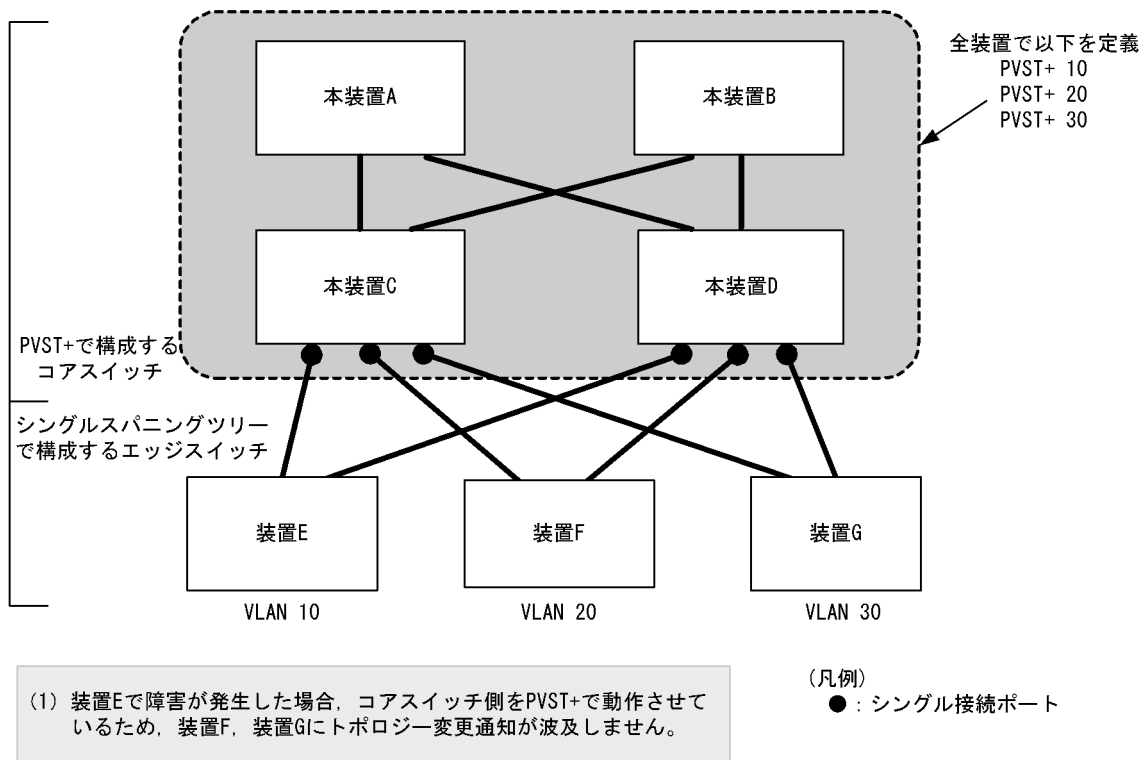
（1）解説

シングルスパニングツリーを使用している装置，または装置で一つのツリーを持つシングルスパニングツリーに相当する機能をサポートしている装置（以降，単にシングルスパニングツリーと表記します。）とPVST+ を用いてネットワークを構築することができます。シングルスパニングツリーで運用している装置をエッジスイッチ，本装置をコアスイッチに配置して使います。このようなネットワークを構築することで，次のメリットがあります。

- エッジスイッチに障害が発生しても，他のエッジスイッチにトポロジー変更の影響が及ばない
- コアスイッチ間でロードバランスできる

● シングルスパニングツリーと接続できるポートの条件
　一つの VLAN にしか定義 (デフォルト VLAN に自動加入しているポートを除く) されてない，かつ untagged-port 定義しているポート。このようなポートをシングル接続ポートと呼びます。

構成例を次の図に示します。この例では，エッジスイッチでシングルスパニングツリーを動作させ，コア - エッジ間の接続を一つの VLAN だけで untagged-port 定義しています。各エッジスイッチはそれぞれ単一の VLAN を定義しています。コアスイッチでは，本装置の PVST+ を動作させています。

図 8-7　シングルスパニングツリーとの接続

（2）シングル接続ポートでシングルスパニングツリーを混在させた場合

PVST+ とシングルスパニングツリーを混在して定義している場合，シングル接続ポートでは，シングルスパニングツリーを停止状態 (Disable) にします。

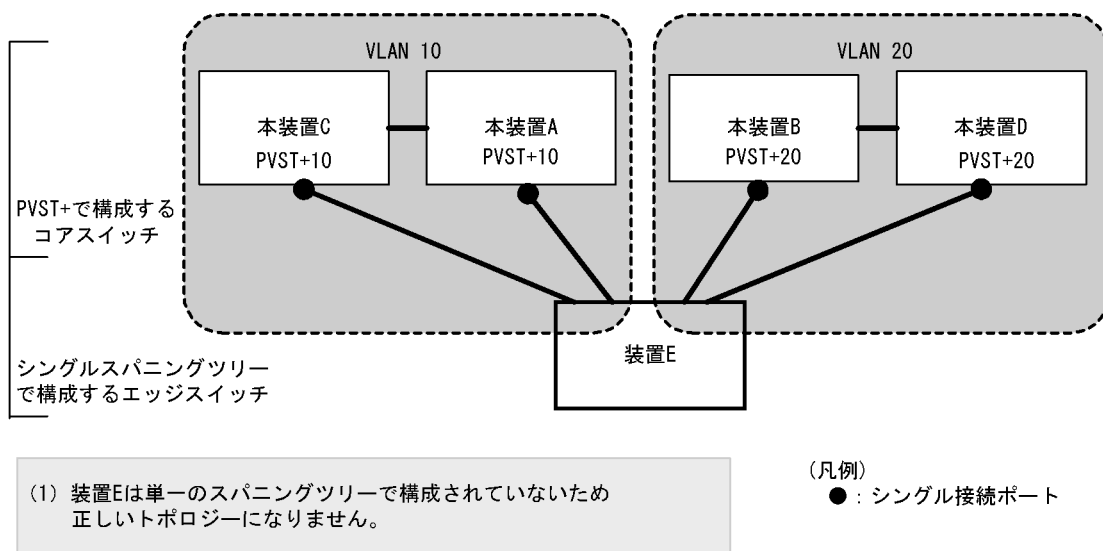
(3) 構成不一致検出機能

同一 VLAN で接続しているポートについて，本装置で untagged-port 定義し，対向装置では tagged-port 定義した場合，当該 VLAN では通信できないポートとなります。このようなポートを構成不一致として検出します。検出する条件は，本装置がシングル接続ポートの場合で，対向装置で tagged-port 定義を設定した場合です。この場合，当該ポートを停止状態 (Disable) にします。対向装置で tagged-port 定義を削除すれば，hello-time 定義の値× 3 秒 (デフォルトは 6 秒) 後に，自動的に停止状態を解除します。

(4) 禁止構成

本装置とシングルスパニングツリーで動作する装置は，単一のスパニングツリーで構成してください。複数のスパニングツリーで構成すると正しいトポロジーになりません。

禁止構成の例を次の図に示します。この例では，装置 E のシングルスパニングツリーが複数の PVST+ スパニングツリーとトポロジーを構成しているため，正しいトポロジーになりません。

図 8-8　シングルスパニングツリーとの禁止構成例

8.4　マルチプルスパニングツリー

8.4.1　概要

マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

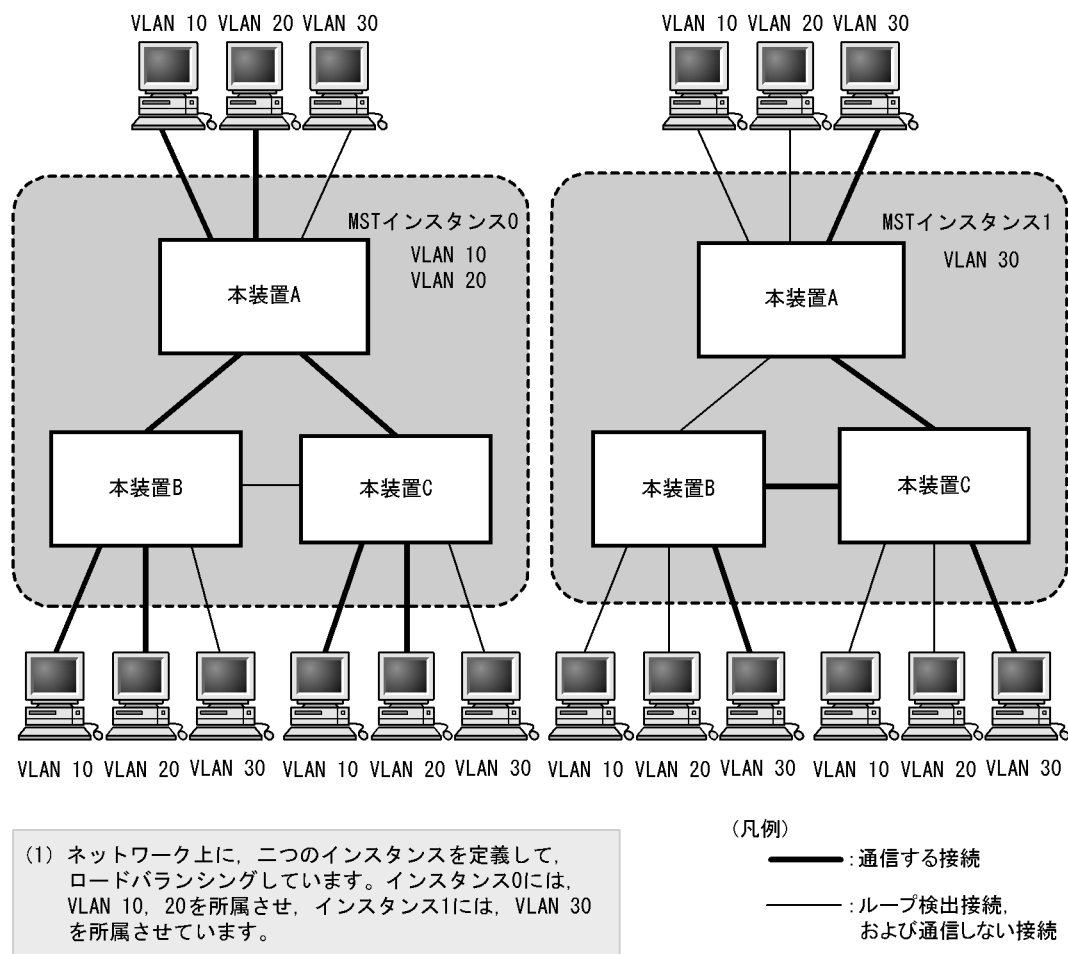
(1) MST インスタンス

マルチプルスパニングツリーは，複数の VLAN をまとめた MST インスタンス (MSTI:Multiple Spanning Tree Instance) というグループごとにスパニングツリーを構築でき，MST インスタンスごとにロードバランシングが可能です。PVST+ によるロードバランシングでは，VLAN 数分のツリーが必要でしたが，マルチプルスパニングツリーでは MST インスタンスによって，計画したロードバランシングに従ったツリーだけで済みます。その結果，PVST+ とは異なり VLAN 数の増加に比例した CPU 負荷およびネットワーク負荷の増加を抑えることができます。

本装置では最大 16 個の MST インスタンスが定義可能です。

MST インスタンスイメージを次の図に示します。

図 8-9　MST インスタンスイメージ

（1）ネットワーク上に，二つのインスタンスを定義して，ロードバランシングしています。インスタンス0には，VLAN 10，20を所属させ，インスタンス1には，VLAN 30を所属させています。

（2） MST リージョン

マルチプルスパニングツリーでは，複数の装置をグルーピングして MST リージョンとして扱うことが可能です。同一の MST リージョンに所属させるには，リージョン名，リビジョン番号，MST インスタンス番号と VLAN の対応を同じにする必要があります。これらはコンフィグレーションで設定します。ツリーの構築は MST リージョン間と MST リージョン内で別々に行い，MST リージョン内のトポロジーは MST インスタンス単位に構築できます。

以下に，MST リージョン間や MST リージョン内で動作するスパニングツリーについて説明します。

● CST

CST(Common Spanning Tree) は，MST リージョン間や，シングルスパニングツリーを使用しているブリッジ間の接続を司るスパニングツリーです。このトポロジーはシングルスパニングツリーと同様で物理ポートごとに計算するのでロードバランシングすることは出来ません。

● IST

IST(Internal Spanning Tree) は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジーのことを指し，MST インスタンス番号 0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

● CIST

CIST(Common and Internal Spanning Tree) は，IST と CST とを合わせたトポロジーを指します。

マルチプルスパニングツリー概要を次の図に示します。

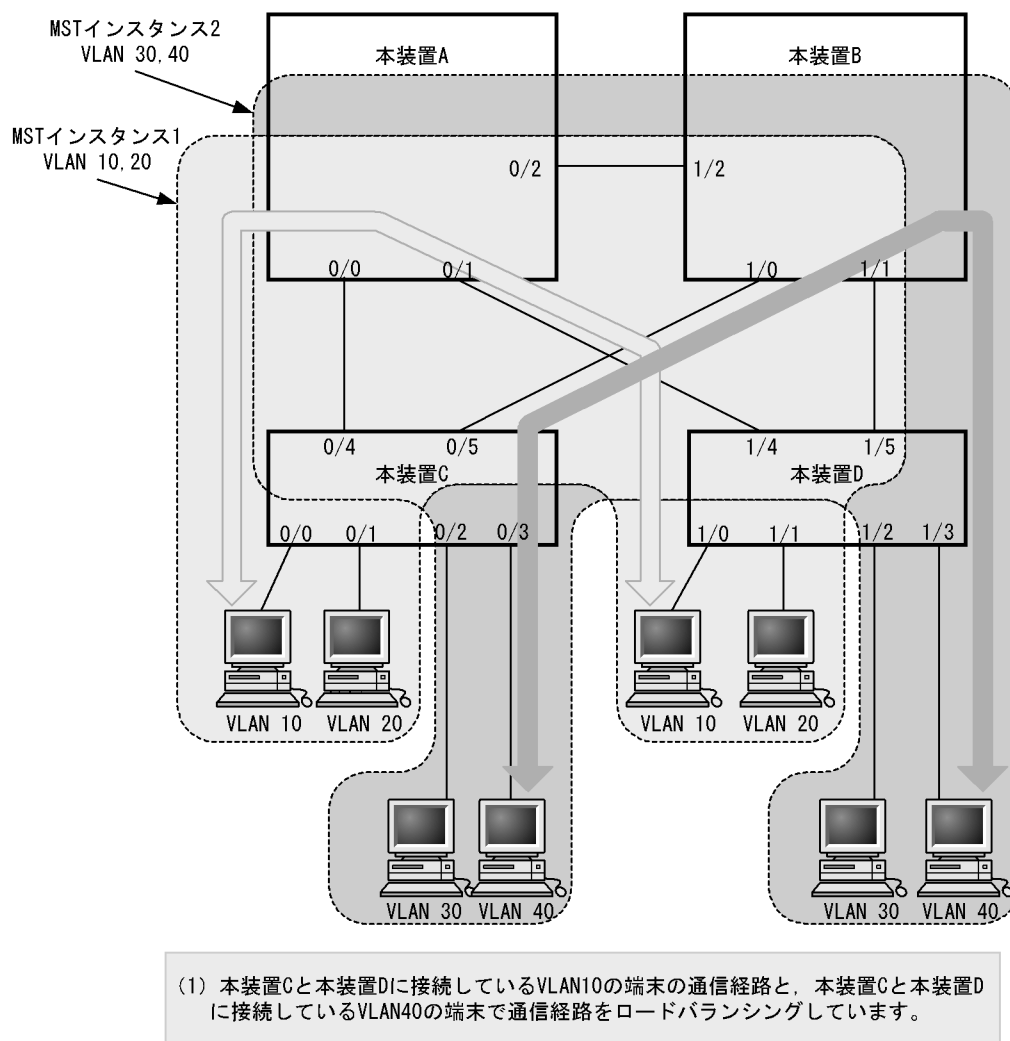
図 8-10　マルチプルスパニングツリー概要

8.4.2　マルチプルスパニングツリーのネットワーク設計

（1）MST インスタンス単位のロードバランシング構成

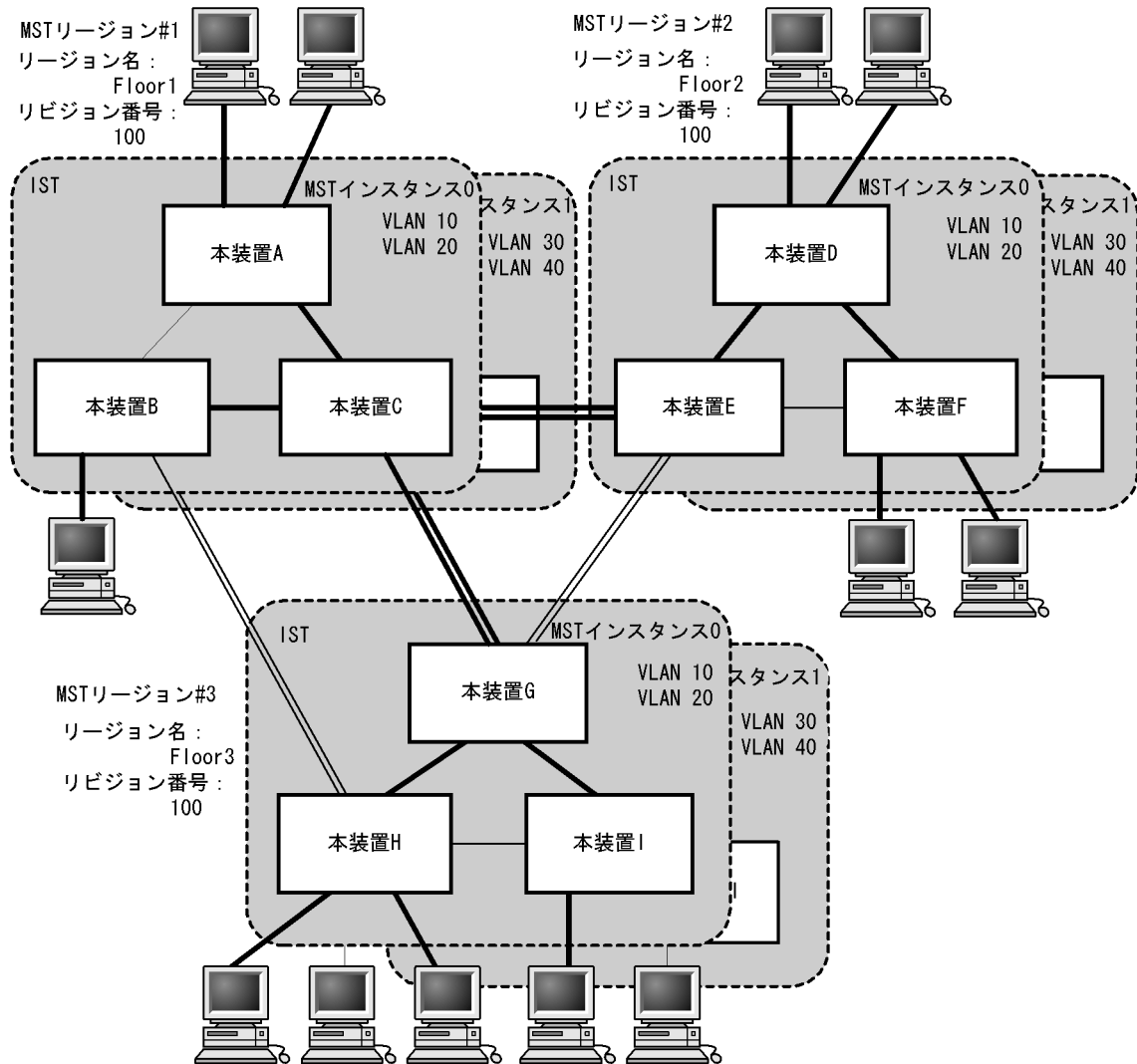
マルチプルスパニングツリーでは，MST インスタンス単位にロードバランシングが可能です。ロードバランシング構成の例を次の図に示します。この例では，VLAN 10，20 を MST インスタンス 1 に，VLAN 30，40 を MST インスタンス 2 に設定して，二つのロードバランシングを行っています。PVST+ では，

この例のように 2 通りのロードバランシングであっても VLAN 数分の 4 つのツリーが必要となります。

図 8-11 ロードバランシング構成

(2) MST リージョンによるネットワーク設計

ネットワーク構成が大規模になるに従ってネットワーク設計は複雑になりますが，MST リージョンによって中小規模構成に分割することで，例えば，ロードバランシングを MST リージョン単位に実施できるため，ネットワーク設計が容易になります。

次の図に MST リージョンによるネットワーク設計例を示します。この例では，装置 A，B，C を MST リージョン #1，装置 D，E，F を MST リージョン #2，本装置 G，H，I を MST リージョン #3 に設定して，ネットワークを三つの MST リージョンに分割しています。

図 8-12　MST リージョンによるネットワーク構成

8.4.3　ほかのスパニングツリーとの互換性

(1)　シングルスパニングツリーとの互換性

マルチプルスパニングツリーは，シングルスパニングツリー上で動作する IEEE802.1D と IEEE802.1w と互換性があります。

IEEE802.1D で動作する装置と接続した場合，別の MST リージョンと判断し，IEEE802.1D 互換モードで動作するため高速遷移しません。

IEEE802.1w で動作する装置と接続した場合，別の MST リージョンと判断し接続します。

(2) PVST+ との互換性

マルチプルスパニングツリーは，PVST+ と互換性はありません。ただし，PVST+ が動作している装置のUntagged ポート（ポート VLAN の Untagged ポートを一つだけ設定しているポート）はシングルスパニングツリーと同等の動作をするため，マルチプルスパニングツリーと接続できます。

8.5　スパニングツリー共通機能

8.5.1　エッジポート

（1） 概要

エッジポートは，端末が接続されループが発生しないことがあらかじめ分かっているポートのための機能です。エッジポートはスパニングツリーのトポロジー計算対象外となり，リンクアップ後，直ちに通信可状態になります。

（2） エッジポートでの BPDU 受信

エッジポートでは BPDU を受信しないことを想定していますが，もし，エッジポートで BPDU を受信した場合は，エッジポートの先にスイッチが存在しループの可能性があることになります。そのため，エッジポートとしての機能を停止し，トポロジー計算や BPDU の送受信など通常のスパニングツリー対象のポートとしての動作を開始します。

いったんスパニングツリー対象のポートとして動作を開始した後，リンクのダウン／アップにより再びエッジポートに戻ります。

（3） エッジポートでの BPDU 送信

エッジポートではスパニングツリーを動作させないため，BPDU の送信は行いません。

ただし，エッジポート同士を誤って接続した状態を検出するために，エッジポートとして即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

（4） エッジポートでの BPDU フィルタ

エッジポートに適用する機能として，BPDU フィルタ機能があります。BPDU フィルタ機能を適用したポートでは，BPDU の送受信を停止します。BPDU の送受信を再開したい場合は本機能を停止してください。

（5） エッジポートでの BPDU ガード機能

エッジポートに適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートでは，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを閉塞します。

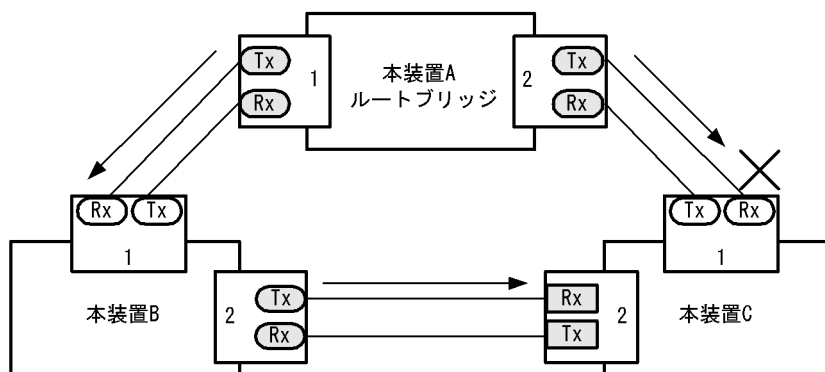
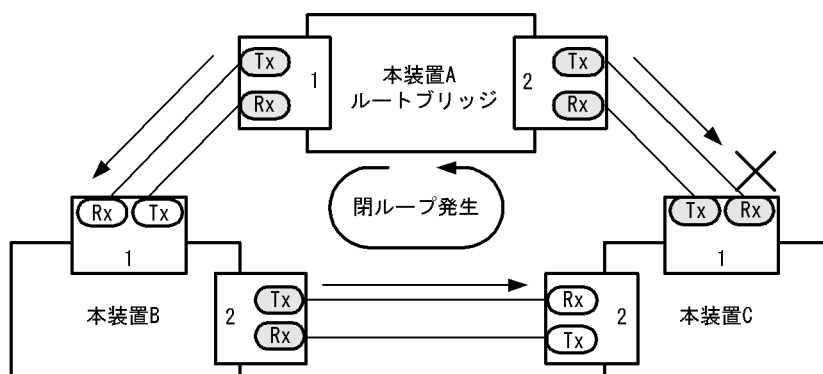
閉塞したポートを free コマンドで解放することによって，再び BPDU ガード機能を適用したエッジポートとしてリンクアップし通信を開始します。

8.5.2　ループガード

（1） 概要

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生する場合があります。次の図に単一方向のリンク障害時の問題点を示します。

図 8-13　単一方向のリンク障害時の問題点

（1）本装置Cのポート1の片リンク故障で，BPDUの受信が途絶えるとルートポートがポート2に切り替わります。

（2）本装置Cのポート1は指定ポートとなって，通信可状態を維持するため閉ループが発生します。

（凡例）　：ルートポート　　：指定ポート　　：非指定ポート

本装置ではループガード機能を用いてループの発生を防止します。

ループガード機能とは BPDU の受信が途絶えたポートの状態を，再度 BPDU を受信するまで転送不可状態に遷移させる機能です。BPDU 受信を開始した場合には通常のスパニングツリー対象のポートとしての動作を開始します。

ループガード機能は，端末を接続するポートを指定する機能であるエッジポートと同じポートに設定することはできません。

8.5.3　ルートガード

（1） 概要

ネットワークの管理の届かない個所で誤って装置が接続された場合や設定が変更された場合，意図しないトポロジーになることがあります。意図しないトポロジーのルートブリッジの性能が低い場合，トラフィックが集中するとネットワーク障害を起こすおそれがあります。ルートガード機能は，このような場合にルートブリッジの候補を特定しておくことによって，ネットワーク障害を回避する機能です。

誤って装置が接続されたときの問題点を次の図に示します。

● 本装置 A，本装置 B をルートブリッジの候補として運用。

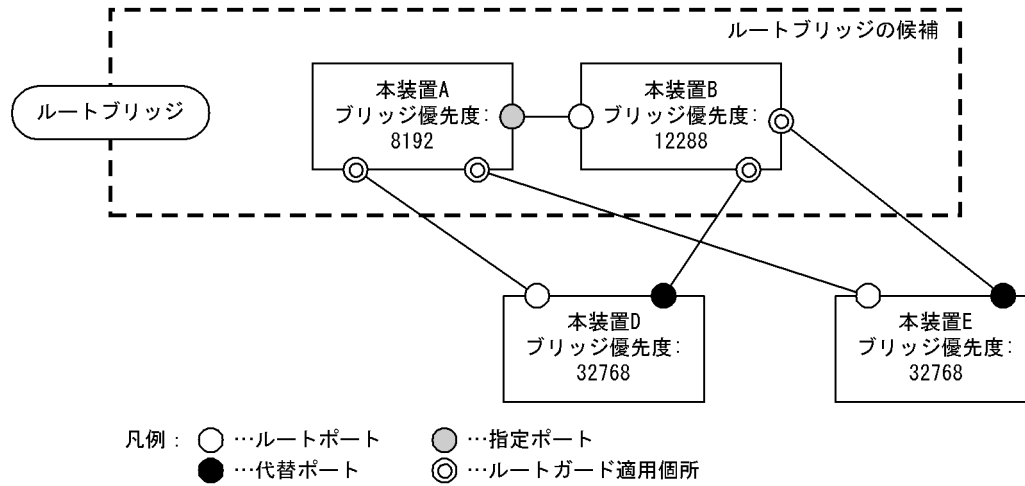
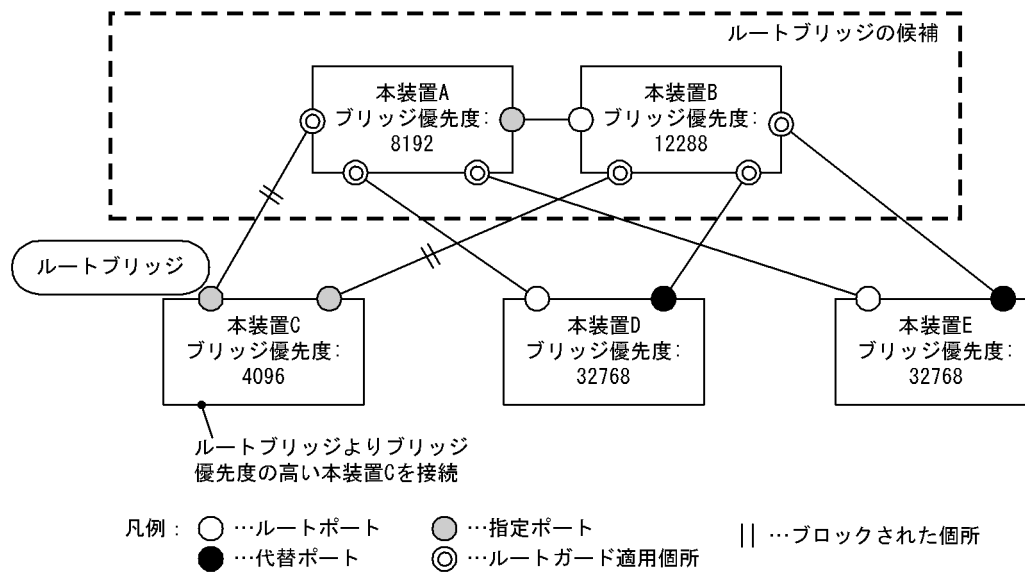
図 8-14　本装置 A，本装置 B をルートブリッジの候補として運用

● 本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続すると，本装置 C がルートブリッジになり，本装置 C にトラフィックが集中するようになる。

図 8-15　本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続

ルートガード機能は，現在のルートブリッジよりも優先度の高いブリッジを検出し，BPDU を廃棄することによってトポロジーを保護します。また，該当するポートをブロック状態に設定することでループを回避します。ルートガード機能は，ループガード機能を設定したポートには設定できません。

8.6 スパニングツリー使用時の注意事項

(1) マルチプルスパニングツリー使用時の注意事項

(a) MST リージョンについて

- 複数の装置を同じ MST リージョンにするためには，該当装置は同じ MST コンフィギュレーションにする必要があります。リージョン名，リビジョン番号，MST インスタンス番号と VLAN の対応を同じにしてください。
- 本装置は 1 ～ 4,095 の VLAN をサポートしていますが，他装置が扱える VLAN の範囲が本装置と異なることがあります。そのような装置を同じ MST リージョンとして扱いたい場合は，該当 VLAN を MST インスタンス 0 に所属させてください。

(b) トポロジーの収束に時間が掛かる場合について

CIST のルートブリッジまたは MST インスタンスのルートブリッジで，次の表に示すイベントが発生すると，トポロジーが落ち着くまでに時間が掛かる場合があります。その間，通信が途絶えたり，FDB のクリアが発生したりします。

イベント	内容	イベントの発生したルートブリッジ種別	影響トポロジー
コンフィグレーション変更	リージョン名 (1)，リビジョン番号 (2)，またはインスタンス番号 (3) と VLAN の対応 (4) をコンフィグレーションで変更し，リージョンを分割または同じにする場合 (1) spanning-tree mst の name サブコマンド (2)spanning-tree mst の revision サブコマンド (3)spanning-tree mst の instance サブコマンド (4)spanning-tree mst instance の instance-vlan サブコマンド	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	ブリッジ優先度を spanning-tree mst instance の bridge-priority サブコマンドのコンフィグレーションで下げた（現状より大きな値を設定した）場合	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	現在の装置の MAC アドレスより値が小さくなるようにコンフィグレーションコマンド local-mac-address で設定した場合	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
二重化 BCU の系切替※	BCU の系切替後に，装置の MAC アドレスの値が小さくなった場合【**SB-7800S**】	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス

イベント	内容	イベントの発生したルートブリッジ種別	影響トポロジー
その他	本装置が停止した場合	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	本装置と接続している対向装置で，ループ構成となっている本装置の全回線がダウンした場合（本装置が当該ループ構成上ルートブリッジではなくなった場合）	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス

注※　実施時の回避策
コンフィグレーションコマンド local-mac-address を設定し，運用系と待機系の MAC アドレスを同じ値に設定してください。

(c) ループガード機能ついて

マルチプルスパニングツリーでループガード機能を使用することはできません。

(2) BCU 二重化構成で BPDU ガード機能を使用する場合について

BPDU ガード機能によってポートがダウンした場合，BCU 障害などで BCU 切り替えが発生すると，新運用系で当該ポートがダウンしたままになります。この状態でコマンドによってスパニングツリーの状態を出力すると，BPDU ガードでポートがダウンしたのではなく，最初からポートがダウンしていたように出力されます。その場合，free コマンドによって当該 Line を運用状態にしてください。

(3) ループガード機能を設定するポートについて

ループガード機能を設定したあと，次に示すイベントが発生すると，ループガードが動作してポートをブロックします。その後，BPDU を受信するまで，ループガードは解除されません。

- 装置起動
- 系切替
- ポートのアップ（リンクアグリゲーションのアップも含む）
- スパニングツリープログラムの再起動
- スパニングツリープロトコルの種別変更（STP/ 高速 STP，PVST+/ 高速 PVST+）

なお，ループガード機能は，指定ポートだけでなく対向装置にも設定してください。指定ポートだけに設定すると，上記のイベントが発生しても，指定ポートは BPDU を受信しないことがあります。このような場合，ループガードの解除に時間が掛かります。ループガードを解除するには，対向装置のポートで BPDU 受信タイムアウトを検出したあとの BPDU の送信を待つ必要があるためです。

また，両ポートにループガードを設定した場合でも，指定ポートで BPDU を一度も受信せずに，ループガードの解除に時間が掛かることがあります。具体的には，対向ポートが指定ポートとなるようにブリッジやポートの優先度，パスコストを変更した場合です。対向ポートで BPDU タイムアウトを検出し，ループガードが動作します。このポートが指定ポートになった場合，BPDU を受信しないことがあり，ループガードの解除に時間が掛かることがあります。

運用中にループガード機能を設定した場合，その時点では，ループガードは動作しません。運用中に設定したループガードは，BPDU の受信タイムアウトが発生した時に動作します。

本装置と対向装置のポート間に BPDU を中継しない装置が存在し，かつポートの両端にループガード機能を設定した状態でポートがリンクアップした場合，両端のポートはループガードが動作したままになります。復旧するには，ポート間に存在する装置の BPDU 中継機能を有効にし，再度ポートをリンクアップさせる必要があります。

（4） VLAN トンネリングについて

VLAN トンネリング設定時，Untagged ポート（VLAN トンネリングのアクセス回線側）はスパニングツリーの対象外になります。Tagged ポート（バックボーン回線側）だけがスパニングツリーを使用できます。

（5） プライベート VLAN について

プライベート VLAN でスパニングツリーを使用する場合，次に示す注意事項があります。

- PVST+ の場合，プライベート VLAN を構成する各 VLAN で PVST+ を使用してください。
- マルチプルスパニングツリーの場合，プライベート VLAN を構成する各 VLAN を異なる MST インスタンスに設定すると，トポロジーによっては通信できない組み合わせができる可能性があります。プライベート VLAN を構成する VLAN はすべて同じ MST インスタンスに設定してください。

（6） BCU の過負荷について

BCU が過負荷な状態となった場合，本装置が送受信する BPDU の廃棄が発生し，タイムアウトのメッセージ出力，トポロジー変更，一時的な通信断となることがあります。

9 IGMP snooping/MLD snooping

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping について説明します。

9.1 IGMP snooping/MLD snooping の概説

この節では，マルチキャスト，IGMP snooping および MLD snooping の概要について説明します。

9.1.1 マルチキャスト概要

同一の情報を複数の受信者に送信する場合，ユニキャストでは送信者が受信者の数だけデータを複製して送信するため，送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してデータを送信します。送信者は受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷を軽減できます。マルチキャスト概要を次の図に示します。

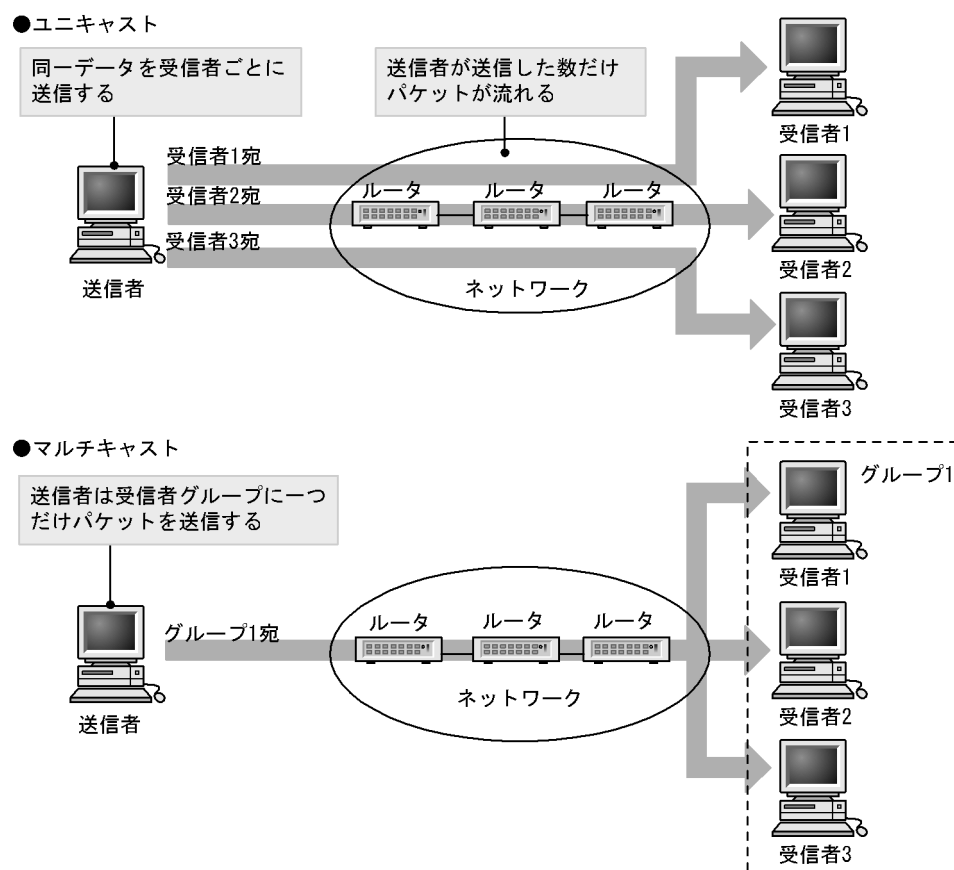
図 9-1　マルチキャスト概要

マルチキャストで送信する場合に，宛先アドレスにはマルチキャストグループアドレスを使用します。マルチキャストグループアドレスを次の表に示します。

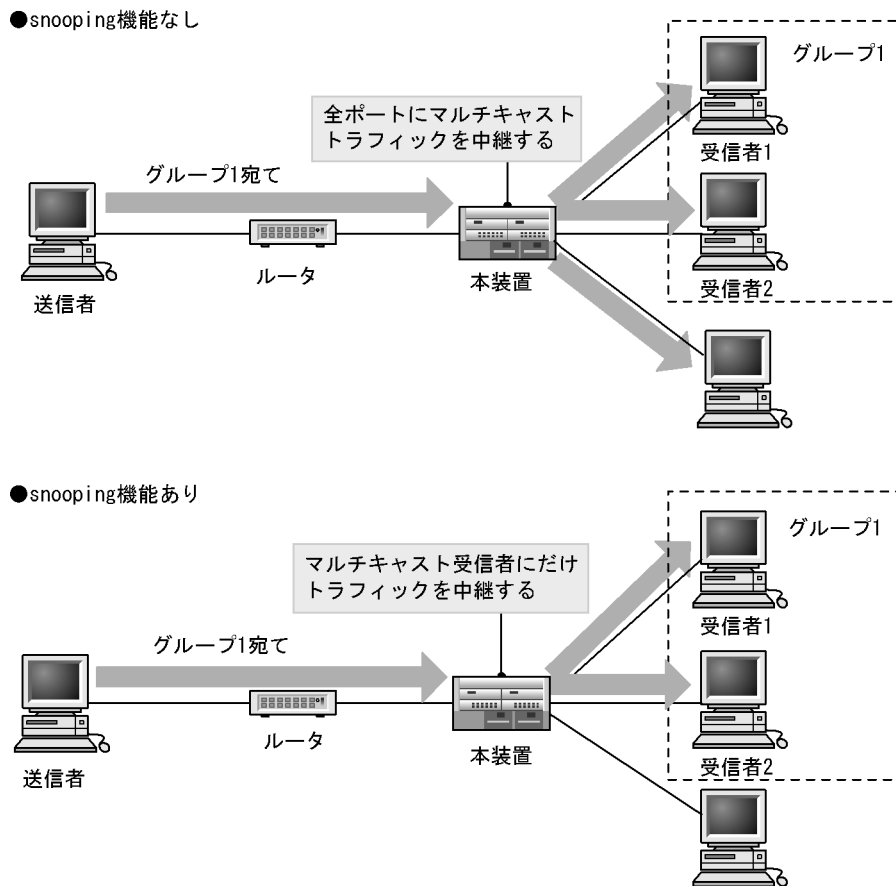
表 9-1　マルチキャストグループアドレス

プロトコル	アドレス範囲
IPv4	224.0.0.0 ～ 239.255.255.255
IPv6	上位 8 ビットが FF(16 進数) となる IPv6 アドレス

9.1.2 IGMP snooping および MLD snooping 概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。このため，レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると，マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れることになります。

IGMP snooping および MLD snooping は，IGMP あるいは MLD メッセージを監視して，受信者が接続しているポートに対してマルチキャストトラフィックを中継します。この機能を利用することで，不要なマルチキャストトラフィックの中継を抑止し，ネットワークを効率的に利用することができます。IGMP snooping/MLD snooping 概要を次の図に示します。

図 9-2 IGMP snooping/MLD snooping 概要

マルチキャストトラフィックの受信者が接続するポートを検出するため，本装置はグループ管理プロトコルのパケットを監視します。グループ管理プロトコルは，ルータホスト間でグループメンバシップ情報を送受信するプロトコルで，IPv4 ネットワークでは IGMP が使用され，IPv6 ネットワークでは MLD が使用されます。ホストから送信されるグループ参加・離脱報告を示すパケットを検出することで，どの接続ポートへマルチキャストトラフィックを中継すべきかを学習します。

9.2　サポート機能

本装置がサポートする IGMP snooping/MLD snooping 機能を次の表に示します。

表 9-2　サポート機能

項 目		サポート内容	備考
インタフェース種別		全イーサネットをサポート フレーム形式は Ethernet V2 だけ	-
		POS（OC-48 および OC-192）は未サポート **【SB-7800S】**	-
		RM イーサネット（SB-5400S ではリモートマネージメントポート）は未サポート	-
IGMP サポートバージョン MLD サポートバージョン		IGMP: Version 1，2，3 MLD: Version 1，2	-
この機能による学習	IPv4	01:00:5e:00:00:00 ～ 01:00:5e:ff:ff:ff	RFC1112 を参照
MAC アドレス範囲	IPv6	33:33:00:00:00:00 ～ 33:33:ff:ff:ff:ff	RFC2464 を参照
IGMP クエリア MLD クエリア		クエリア動作は IGMPv2/IGMPv3，MLDv1/MLDv2 の仕様に従う	-
マルチキャストルータ接続ポートの設定		コンフィグレーションによる static 設定	-

（凡例）-：該当なし

9.3 IGMP snooping

ここでは，IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイマは RFC2236 に従います。また，IGMP バージョン 3（以降，IGMPv3）メッセージのフォーマットおよび設定値は RFC3376 に従います。

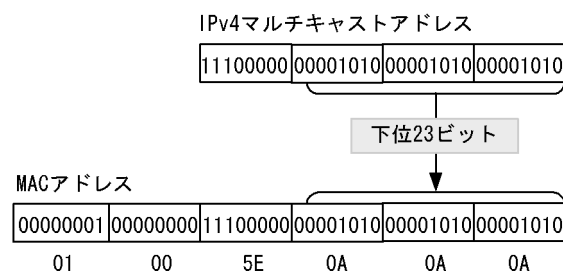
9.3.1 MAC アドレスの学習

IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは FDB に登録します。

(1) エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび IGMPv3 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛のトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 01:00:5E:0A:0A:0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛のパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 9-3 IPv4 マルチキャストアドレスと MAC アドレスの対応

(2) エントリの削除

学習したマルチキャスト MAC アドレスは次のどれかの場合に，すべてのポートにグループメンバが存在しなくなった時点で削除されます。

- IGMPv2 Leave メッセージを受信した場合
  IGMPv2 Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します)。VLAN 内のすべてのポートにグループメンバが存在しなくなった場合にエントリ自体を削除します。
- IGMPv3 Report（離脱要求）メッセージを受信した場合
  IGMPv3 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこの

ポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します)。VLAN内のすべてのポートにグループメンバが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report を受信した場合は，次の条件をすべて満たした場合だけ，Group-Specific Query メッセージの送信およびエントリの削除処理を実行します。
- 自装置にクエリア設定をしている
- 該当する VLAN に IPv4 マルチキャストを使用していない

- IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信してから一定時間経過した場合
マルチキャストルータは直接接続するインタフェース上にグループメンバが存在するかを確認するため，定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合，VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
本装置ではエントリを削除するタイムアウト時間を 260 秒（デフォルト値）としています。260 秒間 IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。タイムアウト時間は次に示す場合に，動的に設定します。
  - 他装置が代表クエリア（IGMPv3 での運用）
  代表クエリアからの IGMPv3 Query メッセージ（QQIC フィールド）から算出します。
  - 自装置が代表クエリアで IPv4 マルチキャストを使用
  IGMPv2/IGMPv3 に関係なく，自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければ，デフォルト値での運用となります)。
  - 他装置が代表クエリア（IGMPv2 での運用）で IPv4 マルチキャストを使用
  該当する VLAN に IPv4 マルチキャストを使用していれば，自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければデフォルト値での運用となります)。

  また，次の場合，タイムアウト時間はデフォルト値での運用となります。
  - 自装置が代表クエリアで IPv4 マルチキャストは未使用
  IGMPv2/IGMPv3 に関係なく，デフォルト値での運用となります。
  - 他装置が代表クエリア（IGMPv2 での運用）で IPv4 マルチキャストは未使用
  該当する VLAN に IPv4 マルチキャストを使用していなければ，デフォルト値での運用となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。
  - 自装置が代表クエリアで IPv4 マルチキャストに DVMRP を使用
  IPv4 マルチキャストに DVMRP を使用している場合，デフォルト値での運用となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。

  注　タイムアウト時間は，Query Interval（QQIC フィールドの値）× 2 ＋ Query Response Interval で算出します。

9.3.2　IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によってレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

「9.3.1　MAC アドレスの学習　(1）エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 01:00:5E:0A:0A:0A となるので，224.10.10.10 宛のマルチキャストデータをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（加入要求）メッセージを受信したポートへも中継します。

9.3.3 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，IGMP はルータホスト間で送受信するプロトコルであるため，IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 9-3　IGMPv1/IGMPv2 メッセージごとの動作

IGMPv1/IGMPv2 メッセージの種類	VLAN 内転送ポート	備考
Membership Query	全ポートへ中継します	-
Version 2 Membership Report	マルチキャストルータポートにだけ中継します	-
Leave Group	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します	※
Version 1 Membership Report	マルチキャストルータポートにだけ中継します	-

（凡例）-：該当なし

注※　自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで IGMPv2 Leave メッセージを受信した場合，クエリアの設定に関係なく IGMPv2 Leave メッセージは中継しません。

表 9-4　IGMPv3 メッセージごとの動作

IGMPv3 メッセージの種類	VLAN 内転送ポート	備考
Version 3 Menbership Query	全ポートへ中継します	-
Version 3 Membership Report	マルチキャストルータポートにだけ中継します	※

（凡例）-：該当なし

注※　加入要求，離脱要求に関係なく IGMPv3 Report はマルチキャストルータポートに中継します。

9.3.4 IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する IGMP Query のバージョンは，IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

9.3.5 同一 VLAN 上での IPv4 マルチキャストが動作する場合

本装置では IPv4 マルチキャストと IGMP snooping の両方を同一の VLAN 上で同時に動作させることが可能です。この場合の動作を次に示します。

1. IPv4 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で IGMP snooping が動作している場合，IGMP snooping の結果によらないでレイヤ 3 中継されたマルチキャストトラフィックは中継先 VLAN 内の全ポートに中継します。
2. IPv4 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，IGMP Leave メッセージ受信によって Group-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

9.4 MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD フレームのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

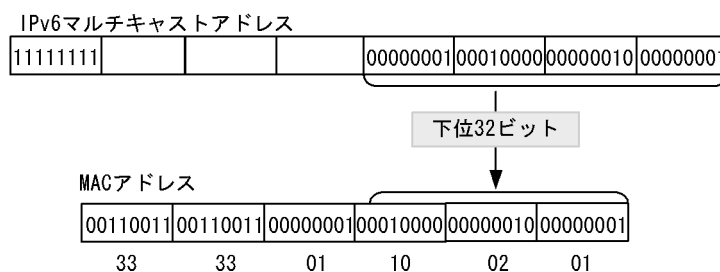
9.4.1 MAC アドレスの学習

MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは FDB に登録します。

(1) エントリの登録

MLDv1 Report メッセージおよび MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛のトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 9-4 IPv6 マルチキャストアドレスと MAC アドレスの対応

(2) エントリの削除

学習したマルチキャスト MAC アドレスは次のどれかの場合に，すべてのポートにグループメンバが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合
  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します)。VLAN 内のすべてのポートにグループメンバが存在しなくなった場合にエントリ自体を削除します。
- MLDv2 Report（離脱要求）メッセージを受信した場合
  MLDv2 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだ

けを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report を受信した場合は，次の条件をすべて満たした場合だけ，Group-Specific Query メッセージの送信およびエントリ削除処理を実行します。
  - 自装置にクエリア設定を行っている
  - 該当する VLAN に IPv6 マルチキャストを使用していない

- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合
マルチキャストルータは直接接続するインタフェース上にグループメンバが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
本装置ではエントリを削除するタイムアウト時間を 260 秒（デフォルト値）としています。260 秒間 MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合に対応するエントリを削除します。
タイムアウト時間は次に示す場合に，動的に設定します。
  - 他装置が代表クエリア（MLDv2 での運用）
  代表クエリアからの MLDv2 Query メッセージ（QQIC フィールド）から算出します。
  - 自装置が代表クエリアで IPv6 マルチキャストを使用
  MLDv1/MLDv2 に関係なく，自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければ，デフォルト値での運用となります）。
  - 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストを使用
  該当する VLAN に IPv6 マルチキャストを使用していれば，自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければデフォルト値での運用となります）。

また，次の場合，タイムアウト時間はデフォルト値での運用となります。
  - 自装置が代表クエリアで IPv6 マルチキャストは未使用
  MLDv1/MLDv2 に関係なく，デフォルト値での運用となります。
  - 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストは未使用
  該当する VLAN に IPv6 マルチキャストを使用していなければ，デフォルト値での運用となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。

注　タイムアウト時間は，Query Interval（QQIC フィールドの値）× 2 ＋ Query Response Interval で算出します。

9.4.2　IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

9.4.3　マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，MLD はルータホスト間で送受信するプロトコルであるため，MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 9-5　MLDv1 メッセージごとの動作

MLDv1 メッセージの種類	VLAN 内転送ポート	備考
Multicast Listner Query	全ポートへ中継します	-
Multicast Listner Report	マルチキャストルータポートにだけ中継します	-
Multicast Listner Done	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します	※

（凡例） -：該当なし

注※　自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで MLDv1 Done メッセージを受信した場合，クエリアの設定に関係なく MLDv1 Done メッセージは中継しません。

表 9-6　MLDv2 メッセージごとの動作

MLDv2 メッセージの種類	VLAN 内転送ポート	備考
Version 2 Multicast Listner Query	全ポートへ中継します	-
Version 2 Multicast Listner Report	マルチキャストルータポートにだけ中継します	※

（凡例） -：該当なし

注※　加入要求，離脱要求に関係なく MLDv2 Report はマルチキャストルータポートに中継します。

9.4.4　MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合，MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する MLD Query のバージョンは，MLDv1 をデフォルト値としています。装置起動以降，

MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

9.4.5 同一 VLAN 上での IPv6 マルチキャストが動作する場合

本装置では IPv6 マルチキャストと MLD snooping の両方を同一の VLAN 上で同時に動作させることが可能です。この場合の動作を次に示します。

1. IPv6 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で MLD snooping が動作している場合，MLD snooping の結果によらないでレイヤ 3 中継されたマルチキャストトラフィックは中継先 VLAN 内の全ポートに中継します。
2. IPv6 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，MLD Done メッセージ受信による Group-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

9.5 IGMP snooping/MLD snooping 使用時の注意事項

(1) 制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。このため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは，VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは，マルチキャスト MAC アドレスの学習結果に従って中継します。

(a) SB-7800S の場合（PSU-1，PSU-2 使用時）

表 9-7　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0 ～ 224.0.0.255
MLD snooping	ff0x:xxxx:xxxx:xxxx:xxxx:xxxx::1 ※ （xxxx：0000 ～ ffff）

注※　MLD snooping を使用する際，宛先 IP アドレスが上表のアドレス範囲外であるルーティングプロトコルの制御パケットは学習されない可能性があるため，マルチキャストルータポートを設定し，制御パケットがルータに転送されるようにしてください。

(b) SB-7800S の場合（PSU-12，PSU-22，PSU-33，PSU-43 使用時）

表 9-8　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0 ～ 224.0.0.255
MLD snooping	ff02::/16

注意

PSU-1，PSU-2 と PSU-12，PSU-22，PSU-33，PSU-43 が混在する構成では，「表 9-5　MLDv1 メッセージごとの動作」および「表 9-6　MLDv2 メッセージごとの動作」に示す動作や，MLDv2 Report の学習などが正常に行われなくなります。そのため，PSU を複数搭載する場合は，装置内のすべての PSU を同じ種類にしてください。PSU-1，PSU-2 と PSU-12，PSU-22，PSU-33，PSU-43 が混在する構成で IGMP snooping/MLD snooping を使用中に，PSU-1，PSU-2 を入れ替えて，PSU-12，PSU-22，PSU-33，PSU-43 だけの構成に変更した場合は，restart snooping コマンドを実行してください。

(c) SB-5400S の場合

表 9-9　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0 ～ 224.0.0.255
MLD snooping	ff02::/16

(2) マルチキャストルータポートの設定

(a) 冗長構成時

スパニングツリーによって冗長構成を採り，スパニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(b) レイヤ2スイッチ間の接続時

複数のレイヤ2スイッチだけで構成されるVLANで，マルチキャストトラフィックの送信ホストを収容するレイヤ2スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成を採る場合は，送信ホストを収容するレイヤ2スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(3) IGMP バージョン3ホストとの接続

本装置にIGMPv3ホストを接続する場合，次に示すどちらかの対応が必要です。

- 該当するVLANにIPv4マルチキャストを使用して，IGMPバージョンを3に設定してください。
- IGMPv3ルータを接続して該当するルータが常に代表クエリアになるようにIPアドレスを設定してください。また，マルチキャストアドレスレコードタイプがBLOCK_OLD_SOURCESのIGMPv3 Reportを受信したときに，本装置が学習しているエントリを削除したい場合は，本装置にもIGMPクエリアを設定してください。この場合も，IGMPv3ルータが代表クエリアになるように設定します。なお，該当するVLANにIPv4マルチキャストを使用しないでください。

(4) MLD バージョン2ホストとの接続

本装置にMLDv2ホストを接続する場合，次に示すどちらかの対応が必要です。

- 該当するVLANにIPv6マルチキャストを使用して，MLDバージョンを2に設定してください。
- MLDv2ルータを接続して該当するルータが常に代表クエリアになるようにIPアドレスを設定してください。また，マルチキャストアドレスレコードタイプがBLOCK_OLD_SOURCESのMLDv2 Reportを受信したときに，本装置が学習しているエントリを削除したい場合は，本装置にもMLDクエリアを設定してください。この場合も，MLDv2ルータが代表クエリアになるように設定します。なお，該当するVLANにIPv6マルチキャストを使用しないでください。

(5) 運用コマンド実行による MAC アドレスの再学習

IGMP/MLD snoopingの運用コマンドのほかに，下記のコマンドを実行した場合，それまでに学習したマルチキャストMACアドレスをクリアし，再学習を行います。運用コマンド実行後は，一時的にマルチキャスト通信が中断します。

- copy backup-config コマンド
- restart vlan コマンド

10 レイヤ 3 インタフェース

この章では，レイヤ 3 中継で使用するインタフェースについて説明します。

10.1　IP アドレスを設定するインタフェース

10.1.1　IP アドレスを設定するインタフェースの種類

本装置で IP アドレスを設定するインタフェースには VLAN やルータポートの Tag-VLAN 連携などがあります。

IP アドレスを設定するインタフェースの種類を次の表に示します。VLAN 以外のインタフェースを設定すると，そのポートはルータポートとなりレイヤ 2 スイッチ機能の対象外になります。詳細については，「6.1.1　概要　(3) スイッチポートとルータポート」を参照してください。

表 10-1　IP アドレスを設定するインタフェースの種類

インタフェース	概要
VLAN	VLAN に対して IP アドレスを設定します。
イーサネット	イーサネットインタフェースに対して直接 IP アドレスを設定します。 ルータポートとなり，イーサネットインタフェースの 1 ポートを単独のインタフェースとして使用できます。 このポートでは VLAN Tag は使用できません。
イーサネット (Tag-VLAN 連携)	イーサネットインタフェースに Tag-VLAN 連携機能を設定し，その VLAN ごとに IP アドレスを設定します。 ルータポートとなり，イーサネットインタフェースの VLAN Tag ごとに異なるインタフェースとして使用できます。 このポートでは，VLAN Tag を使用するインタフェースと，VLAN Tag を使用しない Untagged のインタフェースを両方使用できます。
リンクアグリゲーション	リンクアグリゲーションに対して直接 IP アドレスを設定します。 ルータポートとなり，リンクアグリゲーションの 1 グループを単独のインタフェースとして使用できます。 このポートでは VLAN Tag は使用できません。
リンクアグリゲーション (Tag-VLAN 連携)	リンクアグリゲーションに Tag-VLAN 連携機能を設定し，その VLAN ごとに IP アドレスを設定します。 ルータポートとなり，リンクアグリゲーションの VLAN Tag ごとに異なるインタフェースとして使用できます。 このポートでは，VLAN Tag を使用するインタフェースと，VLAN Tag を使用しない Untagged のインタフェースを両方使用できます。
POS	POS インタフェースに対して IP アドレスを設定します。
トンネルインタフェース	トンネルインタフェースに対して IP アドレスを設定します。
RM イーサネット (SB-5400S ではリモートマネージメントポート)	RM イーサネットに対して IP アドレスを設定します。
メンテナンスポート**【SB-5400S】**	メンテナンスポートに対して IP アドレスを設定します。

10.1.2　インタフェースの MAC アドレス

IP アドレスを設定したインタフェースは，本装置の持つ MAC アドレスの一つをそのインタフェースの MAC アドレスとして使用します。使用する MAC アドレスはインタフェースの種類によって異なります。使用する MAC アドレスを次の表に示します。

装置 MAC アドレスの詳細については，「4.5　本装置の MAC アドレス」を参照してください。

表 10-2 IP アドレスを設定したインタフェースの使用する MAC アドレス

インタフェース	MAC アドレス
VLAN	デフォルトでは，装置 MAC アドレスを使用します。 VLAN ごとの MAC アドレスを使用したい場合は，コンフィグレーションコマンド vlan-mac-prefix および vlan-mac で指定できます。
イーサネット	該当ポートの MAC アドレスを使用します。
イーサネット (Tag-VLAN 連携)	該当ポートの MAC アドレスを使用します。
リンクアグリゲーション	装置 MAC アドレスを使用します。
リンクアグリゲーション (Tag-VLAN 連携)	装置 MAC アドレスを使用します。
POS	-
トンネルインタフェース	-
RM イーサネット (SB-5400S ではリモートマネージメントポート)	該当ポートの MAC アドレスを使用します。
メンテナンスポート**【SB-5400S】**	該当ポートの MAC アドレスを使用します。

（凡例）- : MAC アドレスを使用しません。

VLAN やリンクアグリゲーションのインタフェースの MAC アドレスは，コンフィグレーションによって変更できます。これらを変更すると，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと，本装置の MAC アドレスが不一致となり，一時的に通信ができなくなる場合があるため注意してください。

10.2　Tag-VLAN 連携

(1)　概要

本装置で VLAN Tag を使用したい場合に，VLAN の Tagged ポートとして設定する方法のほかに，一つのポートに Tag-VLAN 連携機能を設定しルータポートとして使用する方法があります。

Tag-VLAN 連携機能を設定したポートはルータポートとなり，VLAN Tag ごとに単独のインタフェースとして動作します。VLAN に二つ以上のポートを必要としない場合，VLAN を設定する代わりに Tag-VLAN 連携機能によって接続できます。Tag-VLAN 連携機能は，ほかの VLAN や Tag-VLAN 連携機能の設定に依存せず自由に VLAN Tag の値を決めることができます。

Tag-VLAN 連携機能は VLAN Tag を使いレイヤ 3 のルーティングを行うもので，VLAN 機能とは異なる機能です。本機能は，管理用ネットワークへの接続やレイヤ 3 機能をサポートしていない LAN スイッチの上位スイッチとしての接続などで，レイヤ 2 スイッチ機能が必要なくレイヤ 3 インタフェースとしてだけ使用したい場合に適用できます。

(2)　サポート仕様

Tag-VLAN 連携のサポート仕様を次の表に示します。

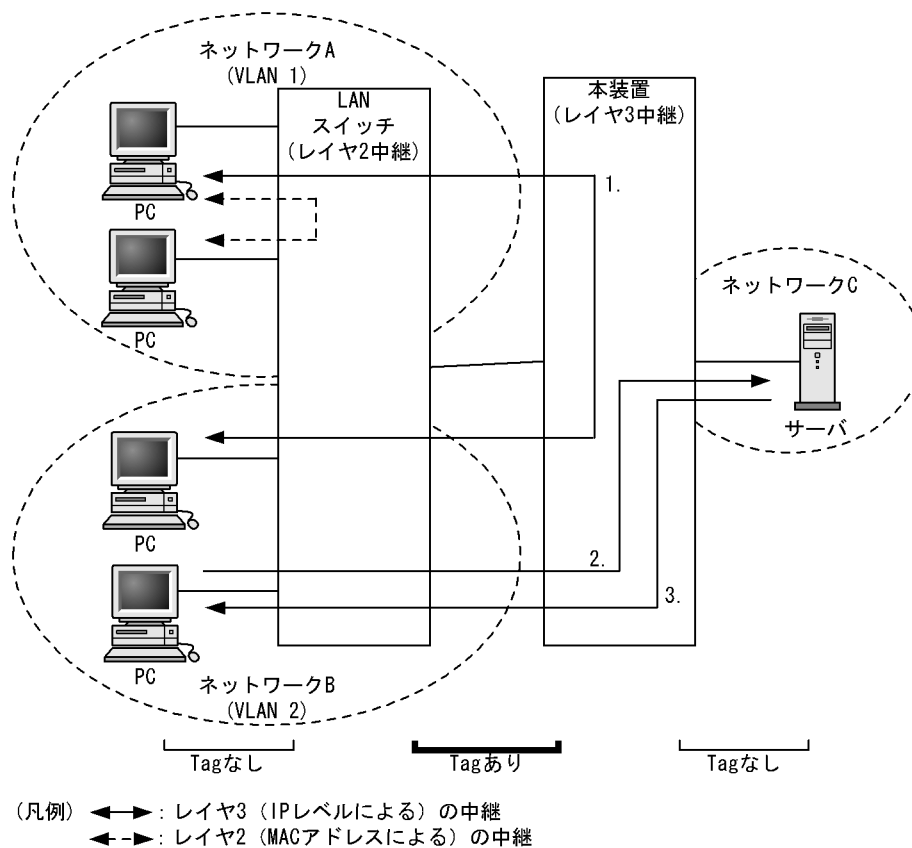
表 10-3　Tag-VLAN 連携サポート仕様

機能	項目	サポート		備考
		IPv4	IPv6	
中継	レイヤ 3 中継	○	○	-
	レイヤ 2 中継	×	×	-
ネットワークインタフェース	イーサネット※	○	○	-
	リンクアグリゲーション	○	○	-
	POS	×	×	-
VLAN 数	ポートまたはリンクアグリゲーション当たりの VLAN 数	4,096(SB-5400S では 1,024)	4,096(SB-5400S では 1,024)	左記の数値は，Tag なしインタフェースを 1 個含みます。
	PSU(SB-5400S では BSU) 当たりの VLAN 数	4,096(SB-5400S では 1,024)	4,096(SB-5400S では 1,024)	-
	装置当たりの VLAN 数	4,096(SB-5400S では 1,024)	4,096(SB-5400S では 1,024)	-
Tag の値	1 ～ 4,095	○	○	-
	Untagged	○	○	同一のポートに Tagged と Untagged を混在できます。
自動設定プロトコル	GVRP	×	×	-
TPID 値	0x8100	○	○	-
	任意の値	○	○	-

（凡例） ○：サポートする ×：サポートしない -：該当しない
注※ Tag-VLAN 連携の設定は RM イーサネットポート（SB-5400S ではリモートマネージメントポート）には設定できません。

(3) ネットワーク構成例

Tag-VLAN 連携を設定することで，一つの物理ポートまたはリンクアグリゲーションに最大 4,096 の VLAN を収容できます。Tag-VLAN 連携のネットワーク構成を次の図に示します。この図の構成では，ネットワーク A（VLAN ID=1）とネットワーク B（VLAN ID=2）を接続しているインタフェースには二つの VLAN を設定します。

図 10-1 Tag-VLAN のネットワーク構成

ネットワーク A からネットワーク B（またはその逆）へフレームを送る場合，ネットワーク B からネットワーク C へフレームを送る場合，本装置による中継はレイヤ 3 中継（異なるサブネット間の中継）になります。

Tag-VLAN 連携がサポートするレイヤ 3 中継の流れを次に示します（番号は「図 10-1 Tag-VLAN のネットワーク構成」に対応しています)。

1. Tag 付きフレームの受信（VLAN ID=1）→ Tag 付きフレームの送信（VLAN ID=2）
2. Tag 付きフレームの受信（VLAN ID=2）→ Tag の削除→ Tag なしフレームの送信
3. Tag なしフレームの受信→ Tag の付加→ Tag ありフレームの送信（VLAN ID=2）

(4) Tag-VLAN 連携使用時の注意事項

1. コンフィグレーションで設定した内容（VLAN ID 指定，または untagged 指定）と異なるパケットを

受信した場合，本装置はそのパケットをハードウェアで廃棄します。Tag-VLAN 連携設定と受信パケット種別を次の表に示します。

表 10-4　Tag-VLAN 連携設定と受信パケット種別

受信パケット		Tag-VLAN 連携設定	
		VLAN ID 指定	untagged 指定
Tagged	設定した VLAN ID	中継	廃棄
	設定していない VLAN ID	廃棄	廃棄
Untagged		廃棄	中継

2. 異なる物理ポートまたはリンクアグリゲーションには Tag-VLAN 連携の設定と非設定は混在できます。Tag-VLAN 連携の VLAN ID として「untagged」を指定すると Untagged のインタフェース，1 ～ 4,095 の値を指定すると Tagged のインタフェースを設定できます。
   ネットワークインタフェースに Tag-VLAN 連携が設定されているかどうかは，ポート単位の場合は show interfaces コマンドで，リンクアグリゲーション単位の場合は show link-aggregation コマンドで確認できます。各コマンドの詳細は，マニュアル「運用コマンドレファレンス Vol.1」を参照してください。

11 IPv4 パケット中継

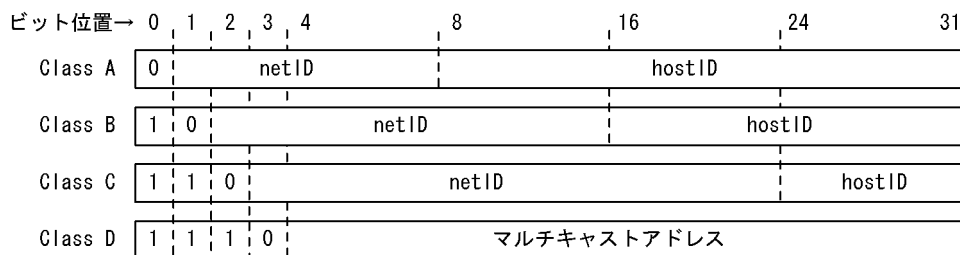
IPv4 ネットワークには通信機能，IP パケット中継，経路制御機能および付加機能があります。この章ではアドレッシングおよび IPv4 パケット中継について説明します。

11.1　アドレッシング

本装置で使用する IP アドレスのアドレッシングについて概要を示します。

11.1.1　IP アドレス

本装置は IP アドレスの Class A，B，C，D をサポートします。Class D はルーティングプロトコルで使用します。使用するルーティングプロトコルに依存しますが，CIDR(Classless Inter-Domain Routing) で規定されているアドレスも使用できます。IP アドレスフォーマットを次の図に示します。

図 11-1　IP アドレスフォーマット

なお，ネットワークブロードキャストアドレスおよびサブネットワークブロードキャストアドレスは，host ID が 2 進数ですべて 1 またはすべて 0 の 2 種類をサポートしており，その選択はインタフェース単位にコンフィグレーションで指定できます。インタフェースについては「11.2.1　IP アドレス付与単位」を参照してください。

本装置に付与する IP アドレスとして次に示す IP アドレスを使用できます。

● net ID

net ID は次の範囲の値を使用できます。

- Class A：1.x.x.x 〜 126.x.x.x
- Class B：128.1.x.x 〜 191.254.x.x
- Class C：192.0.1.x 〜 223.255.254.x　(x=host ID)

● host ID

host ID は次の範囲の値を使用できます。

- Class A：y.0.0.1 〜 y.255.255.254
- Class B：y.y.0.1 〜 y.y.255.254
- Class C：y.y.y.1 〜 y.y.y.254　(y=net ID)

11.1.2　サブネットマスク

「図 11-1　IP アドレスフォーマット」に示す Class A，B，C の net ID，host ID の境界位置に関係なく，サブネットマスクを使用して任意の境界位置に net ID と host ID の境界位置を指定できます。

例えば，Class B の net ID を一つ入手し，それを 256 個のサブネットに分割して使用する場合は，サブネットマスクを 255.255.255.0 とします。また，CIDR に対応した使い方として Class C の連続した二つの net ID(例えば，192.0.0.x と 192.0.1.x) を入手し，それを一つのサブネットワークとして使用する場合は，サブネットマスクを 255.255.254.0 とします。

サブネットマスクはインタフェースごとにコンフィグレーションで左詰め (2 進数表現で上位の桁から '1'

が連続）で指定します。

例えば，サブネットマスクに 255.255.192.0 は設定できますが，255.255.96.0 は設定できません。

11.2　アドレッシングとパケット中継動作

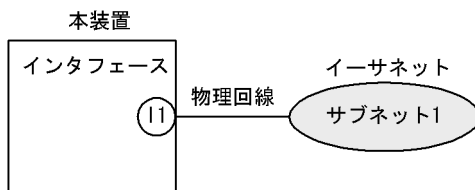
11.2.1　IP アドレス付与単位

本装置で IP アドレスを付与する単位を**インタフェース**と呼びます。最も基本的な接続形態では，回線に接続するポートに対して一つのインタフェースを設定します。1 個のインタフェースに 1 個の IP アドレスを設定します。ただし，例外としてイーサネットのマルチホーム接続では，1 個のインタフェースに複数の IP アドレスを設定できます。

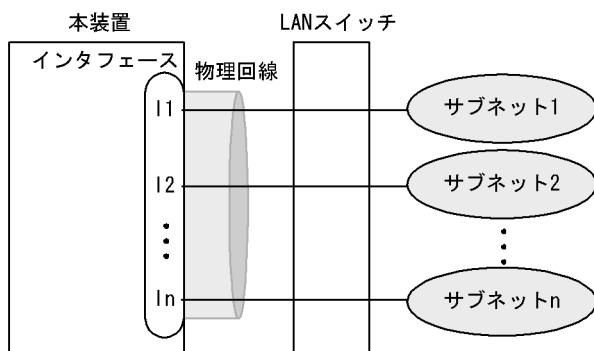
イーサネットのネットワークへの接続形態は，ブロードキャスト型です。一方，トンネルインタフェース，RM イーサネット（SB-5400S ではリモートマネージメントポート）のダイアルアップ IP 接続インタフェースはポイント - ポイント型です。

(1) ブロードキャスト型の接続

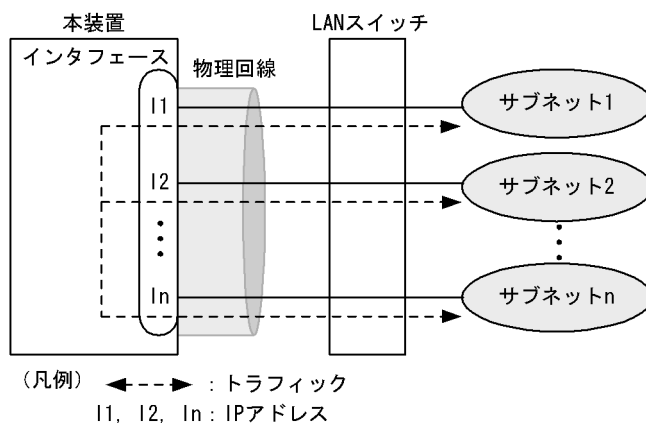
1 インタフェースに対して 1 個の IP アドレスを設定します。したがって，1 物理回線が接続するネットワークが 1 個の IP サブネットになります。インタフェースと IP サブネットの関係を次の図に示します。

図 11-2　インタフェースと IP サブネットの関係 (ブロードキャスト接続)

(2) ブロードキャスト型のマルチホーム接続

一つの物理回線に対して，一つのインタフェースを設定し，さらにそのインタフェースに対して複数の IP アドレスを設定します。これによって，1 物理回線内でのルーティングができます。インタフェースと IP サブネットの関係を次の図に示します。

図 11-3　インタフェースと IP サブネットの関係 (マルチホーム接続)

11.2.2 マルチホーム接続

イーサネットインタフェースでマルチホーム接続時のパケット中継動作を次の図に示します。LAN スイッチ下のサブネット間のパケットを本装置で中継します。

図 11-4 マルチホーム接続時のパケット中継動作

11.3 IP レイヤ機能

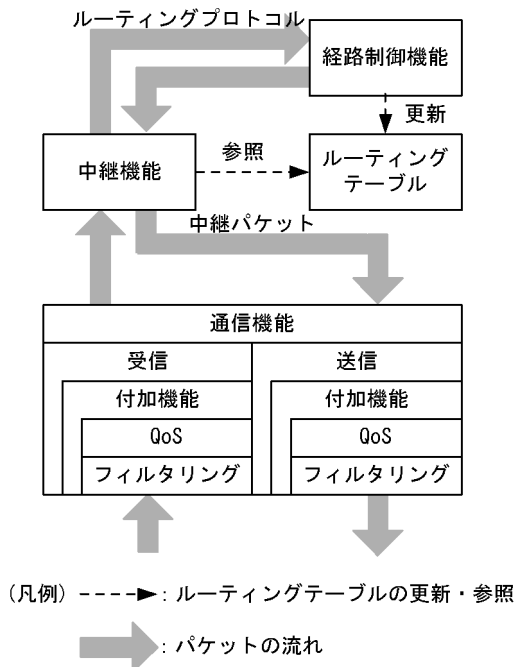
本装置は受信した IP パケットをルーティングテーブルに従って中継します。この中継処理は大きく分けて次の四つの機能から構成されています。

- 通信機能
  IP レイヤの送信および受信処理を行う機能です。
- 中継機能
  ルーティングテーブルに従って IP パケットを中継する機能です。
- 経路制御機能
  経路情報の送受信や，中継経路を決定しルーティングテーブルを作成する機能です。
- 付加機能
  フィルタリングと QoS の機能をサポートします。フィルタリングは特定のパケットを中継または廃棄する機能です。QoS は特定のパケット通信品質を保証する機能です。フィルタリングと QoS は送信と受信の両方の契機で行うことができます。

なお，IP ルーティングのそのほかの機能として，次の機能をサポートしています。

- ロードバランス機能
- Null インタフェース機能
- DHCP/BOOTP リレーエージェント機能

IP ルーティング機能の概念を次の図に示します。

図 11-5 IP ルーティング機能の概念

11.4 通信機能

この節では IPv4 のパケット中継で使用する通信プロトコルについて説明します。IPv4 の通信プロトコルとして，次のプロトコルが使用できます。

- IP
- ICMP
- ARP

11.4.1 インターネットプロトコル (IP)

(1) IP パケットフォーマット

本装置が送信する IP パケットのフォーマットおよび設定値は RFC791 に従います。

本装置がサポートする IP オプションについては「(3) IP オプションサポート仕様」を参照してください。

(2) IP パケットヘッダ有効性チェック

IP パケット受信時に IP パケットのヘッダの有効性チェックを行います。IP パケットヘッダのチェック内容を次の表に示します。

表 11-1 IP パケットヘッダのチェック内容

IP パケットヘッダフィールド	チェック内容	チェック NG 時パケット廃棄	パケット廃棄時 ICMP 送信
バージョン	バージョン＝ 4 であること	○	×
ヘッダレングス	ヘッダレングス≧ 5 であること	○	×
TOS	チェックしない	-	-
トータルレングス	トータルレングス≧ 4 ×ヘッダレングスであること	○	×
パケット識別子	チェックしない	-	-
フラグ	チェックしない	-	-
フラグメントオフセット	チェックしない	-	-
TTL	自装置宛に受信したパケットの TTL : チェックしない	-	-
	フォワーディングするパケットの TTL : TTL-1 ＞ 0 であること	○	○※
プロトコル	チェックしない	-	-
ヘッダチェックサム	ヘッダチェックサムが正しいこと	○	×
送信元アドレス	チェックしない	-	-
宛先アドレス	次の条件をすべて満たすこと 1. クラス A，クラス B，クラス C，クラス D 2. ネットワーク番号が 127(内部ループバックアドレス) でないこと 3. ネットワーク番号が 0 でないこと (ただし，0.0.0.0 を除く)	○	×

(凡例) ○ : 行う　× : 行わない　- : 該当しない

注※　ICMP Time Exceeded メッセージを送信します。

(3)　IP オプションサポート仕様

本装置がサポートする IP オプションを次の表に示します。

表 11-2　IP オプションサポート仕様

IP オプション	IP パケットの分類		
	本装置が発局のパケット	本装置が着局のパケット	本装置が中継するパケット
End of Option List	○	-	-
No Operation	○	-	-
Loose Source Routing	○	○	○
Strict Source Routing	×	○	○
Record Route	○	○	○
Internet Timestamp	×	○	○

(凡例)　○：サポートする　×：サポートしない　-：オプション処理なし

11.4.2　ICMP

(1)　ICMP メッセージフォーマット

本装置が送信する ICMP メッセージのフォーマットおよび設定値は RFC792 に従います。

(2)　ICMP メッセージサポート仕様

ICMP メッセージのサポート仕様を次の表に示します。

表 11-3　ICMP メッセージサポート仕様 (値は 10 進)

<table>
<tr><th colspan="4">ICMP メッセージ</th><th rowspan="3">サポート</th></tr>
<tr><th colspan="2">タイプ (種別)</th><th colspan="2">コード (詳細種別)</th></tr>
<tr><th>-</th><th>値</th><th>-</th><th>値</th></tr>
<tr><td rowspan="11">Destination Unreachable</td><td rowspan="11">3</td><td>Net Unreachable</td><td>0</td><td>○</td></tr>
<tr><td>Host Unreachable</td><td>1</td><td>○</td></tr>
<tr><td>Protocol Unreachable</td><td>2</td><td>○</td></tr>
<tr><td>Port Unreachable</td><td>3</td><td>○</td></tr>
<tr><td>Fragmentation Needed and DF Set</td><td>4</td><td>○</td></tr>
<tr><td>Source Route Failed</td><td>5</td><td>○</td></tr>
<tr><td>Destination Network Unknown</td><td>6</td><td>×</td></tr>
<tr><td>Destination Host Unknown</td><td>7</td><td>×</td></tr>
<tr><td>Network Unreachable for Type of Service</td><td>11</td><td>×</td></tr>
<tr><td>Host Unreachable for Type of Service</td><td>12</td><td>×</td></tr>
<tr><td>Communication Administratively Prohibited</td><td>13</td><td>○</td></tr>
</table>

ICMP メッセージ				サポート
タイプ (種別)		コード (詳細種別)		
-	値	-	値	
		Host Precedence Violation	14	×
		Precedence Cutoff in Effect	15	×
Source Quench	4	-	0	×
Redirect	5	Redirect Datagrams for the Network	0	×
		Redirect Datagrams for the Host	1	○
		Redirect Datagrams for the Type of Service and Network	2	×
		Redirect Datagrams for the Type of Service and Host	3	×
Time Exceeded	11	Time to Live Exceeded in Transit	0	○
		Fragment Reassembly Time Exceeded	1	×
Parameter Problem	12	-	0	○
Echo Request	8	-	0	○
Echo Reply	0	-	0	○
Timestamp Request	13	-	0	×
Timestamp Reply	14	-	0	○※
Information Request	15	-	0	×
Information Reply	16	-	0	×
Address Mask Request	17	-	0	×
Address Mask Reply	18	-	0	○※

(凡例) ○：サポートする　×：サポートしない　-：該当しない

注※　Request メッセージを受信した場合は，Reply メッセージを返します。

(3) ICMP Redirect の送信仕様

次の条件を満たすときに ICMP Redirect のパケットを送信します。

- パケット送信元とネクストホップのルータが同一セグメントにある (受信 IP パケットの送信元 IP アドレスのサブネットワークアドレスと中継先ネクストホップ・アドレスのサブネットワークアドレスが同一)
- 受信パケットが ICMP 以外の IP パケット
- コンフィグレーション IP ルーティング情報で送信有効を指定している

(4) ICMP Time Exceeded の送信仕様

次の条件を満たすときに ICMP Time Exceeded のパケットを送信します。

- フォワーディングする受信 IP パケットの TTL が 1
- 受信パケットが ICMP 以外の IP パケット (ただし，ICMP Echo パケットは除く)

(5) 注意事項

ICMP メッセージは，QoS 制御でのキューイング優先度が最低位のため，回線が過負荷の状態では送信で

きない場合があります。このため，次の現象が発生する要因となります。

- traceroute コマンドの応答がタイムアウトとなる。
- パケット到達不可通知が送出されていない。
- リダイレクト通知が送出されていない。
- フラグメント不可による MTU 長通知が送出されない。

11.4.3 ARP

(1) ARP フレームフォーマット

本装置が送信する ARP フレームのフォーマット，および設定値は RFC826 に従います。

(2) ARP フレーム有効性チェック

本装置は，受信した ARP フレームの有効性をチェックします。ARP フレームのチェック内容を次の表に示します。

表 11-4　ARP フレームのチェック内容

ARP フレームフィールド	チェック内容	フレーム廃棄
ハードウェアタイプ	(イーサネットの場合) ハードウェアタイプ＝ 1(Ethernet) または 6(IEEE 802 Networks) であること	○
プロトコルタイプ	プロトコル＝ 0800H(IP) であること 1000H(Trailer packet) であること※	○
ハードウェアアドレス長	チェックしない	-
プロトコルアドレス長	チェックしない	-
オペレーションコード	オペレーションコード＝ 1(REQUEST)，1 以外は 2(REPLY) と扱う	-
送信元ハードウェアアドレス	以下の値ではないこと • マルチキャストアドレス • ブロードキャストアドレス • 自装置ハードウェアアドレスと同じ	○
送信元プロトコルアドレス	以下の値ではないこと • マルチキャストアドレス • 自装置プロトコルアドレスと同じ • 0.0.0.0	○
宛先ハードウェアアドレス	チェックしない	-
宛先プロトコルアドレス	• 自装置のプロトコルアドレスであること	○

(凡例)　○：チェック NG のときフレームを廃棄する　-：該当しない

注※
「Trailer packet」の自発送信は行いませんが，要求のあった場合は応答を返して学習をします。

(3) ProxyARP

本装置はイーサネットに接続するすべてのインタフェースで ProxyARP を動作させることができます。動作の有無はコンフィグレーションで設定します。本装置は次の条件をすべて満たす ARP 要求パケットを受信した場合に，宛先プロトコルアドレスの代理として ARP 応答パケットを送信します。

- ARP 要求パケットの宛先プロトコルアドレスがブロードキャストアドレスではない

- ARP 要求パケットの送信元プロトコルアドレスと宛先プロトコルアドレスのネットワーク番号が等しい
- ARP 要求パケットの送信元プロトコルアドレスと宛先プロトコルアドレスのサブネットワーク番号が異なる
- ARP 要求パケットの宛先プロトコルアドレスがルーティングテーブルにあり到達できる

(4) エージングタイマ

ARP 情報のエージング時間はインタフェースごとに分単位で指定できます。指定値は最小 1 分で最大 65535 分です。また，デフォルト値は 30 分です。

ARP エントリを多数登録する場合は，ARP キャッシュテーブルエージング時間を極端に短くしないでください。

ARP エントリ数と，ARP キャッシュテーブルエージング時間の最短時間の目安を次の表に示します。

表 11-5 ARP エントリ数と，ARP キャッシュテーブルエージング時間の最短時間の目安【SB-7800S】

ARP エントリ数	0 ～ 5,000	5,001 ～ 20,000	20,001 ～ 35,000	35,001 ～ 50,000	50,001 ～ 65,536(最大値)
最短エージング時間 (分)	1	3	5	7	9

注 最初の 5,000 エントリまでは最短 1 分とし，それ以降は 7,500 エントリを目処に 1 分延ばしてください。

表 11-6 ARP エントリ数と，ARP キャッシュテーブルエージング時間の最短時間の目安【SB-5400S】

ARP エントリ数	0 ～ 5,000	5,001 ～ 20,000	20,001 ～ 32,748(最大値)
最短エージング時間 (分)	1	3	5

注 最初の 5,000 エントリまでは最短 1 分とし，それ以降は 7,500 エントリを目処に 1 分延ばしてください。

(5) ARP 情報の設定

ARP プロトコルを持たない製品を接続するために，イーサネットの場合 MAC アドレスと IP アドレスの対応 (ARP 情報) をコンフィグレーションで設定できます。

(6) ARP 情報の参照

運用端末からコマンドで ARP 情報が参照できます。ARP 情報から該当インタフェースの IP アドレスと MAC アドレスの対応がわかります。

11.5　中継機能

11.5.1　IP パケットの中継方法

中継機能は受信したパケットをルーティングテーブルに従って次のルータまたはホストに転送する処理です。

(1) ルーティングテーブルの内容

ルーティングテーブルは複数個のエントリから構成されており，各エントリは次の内容を含んでいます。本装置のルーティングテーブルの内容はコマンドで表示できます。

Destination：

宛先ネットワークアドレスと宛先ネットワークアドレスに対するサブネットマスクのビット長です。サブネットマスクは，ルーティングテーブル検索時，受信 IP パケットの宛先 IP アドレスに対するマスクになります。サブネットワークに分割されていない宛先ネットワークアドレスについては，そのネットワークアドレスのネットワーククラスに対応したマスクビット長 (例えば，classA なら 8) を表示します。なお，ホストアドレスによる中継を行う場合には 32 を表示します。

Next Hop：

次に中継する必要のあるルータの IP アドレスです。マルチパス機能を使用すると，複数個の Next Hop が存在します。

Interface：Next Hop のあるインタフェース名称です。

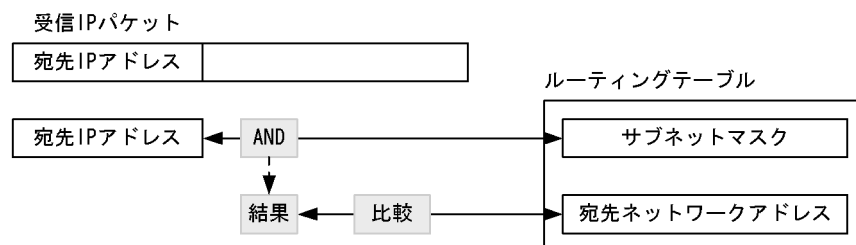
Metric：ルートのメトリックです。

Protocol：学習元プロトコルです。

Age：ルートが確認，または変更されてからの時間 (秒) です。

(2) ルーティングテーブルの検索

受信した IP パケットの宛先 IP アドレスに該当するエントリをルーティングテーブルから検索します。該当するエントリとは，受信した IP パケットの宛先 IP アドレスをルーティングテーブルのサブネットマスクでマスク (AND) を取った結果が宛先ネットワークアドレスと同じ値になるものです。ルーティングテーブルの検索を次の図に示します。

図 11-6　ルーティングテーブルの検索

11.5.2　ブロードキャストパケットの中継方法

本装置では，IP 中継で直接接続するネットワークまたはサブネットワークのブロードキャスト (以降，ダ

イレクトブロードキャスト）パケットを中継するかどうかを制御できます。コンフィグレーションによる 2 種類のブロードキャスト中継スイッチの指定によって行います。一つは，パケットの中継で入力側のインタフェースに適用する **subnetbroad_forward スイッチ**（デフォルト：中継しない）と，もう一つは，出力側のインタフェースにダイレクトのサブネットごとに適用する **directbroad_forward スイッチ**（デフォルト：中継しない）です。

コンフィグレーションで指定しない場合は中継しませんが，中継を指定した場合は，次の図のような端末への攻撃が考えられるため注意が必要となります。

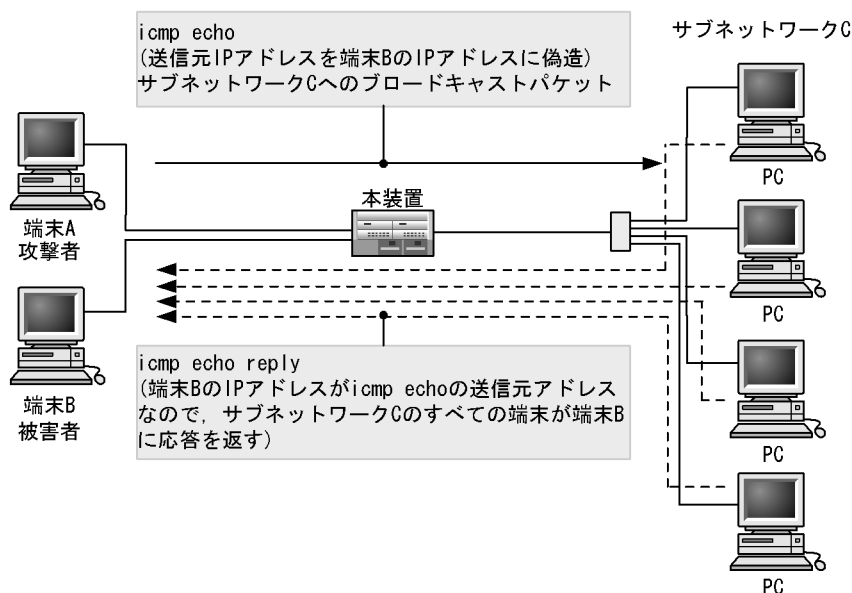
図 11-7　サブネットワークへのブロードキャストパケットを使った攻撃例

directbroad_forward スイッチはアドレスごとに指定できるため，サブネットごとに制御する場合に有効です。通常はこちらを使用することをお勧めします。サブネットワークごとに中継可否を決定する設定例を「図 11-8　サブネットワークごとに中継可否を決定する設定例」に示します。また，両スイッチを指定した場合の組み合わせを「表 11-7　両スイッチを指定した場合の組み合わせ」に示します。

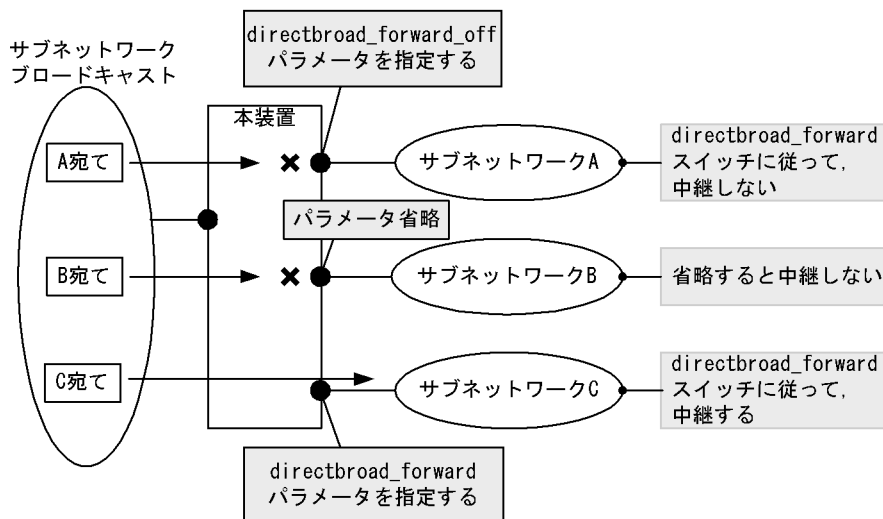
図 11-8　サブネットワークごとに中継可否を決定する設定例

入力インタフェースで中継可否を決定する設定例を「図 11-9　入力インタフェースで中継可否を決定する設定例」に示します。また，両スイッチを指定した場合の組み合わせを「表 11-7　両スイッチを指定した場合の組み合わせ」に示します。

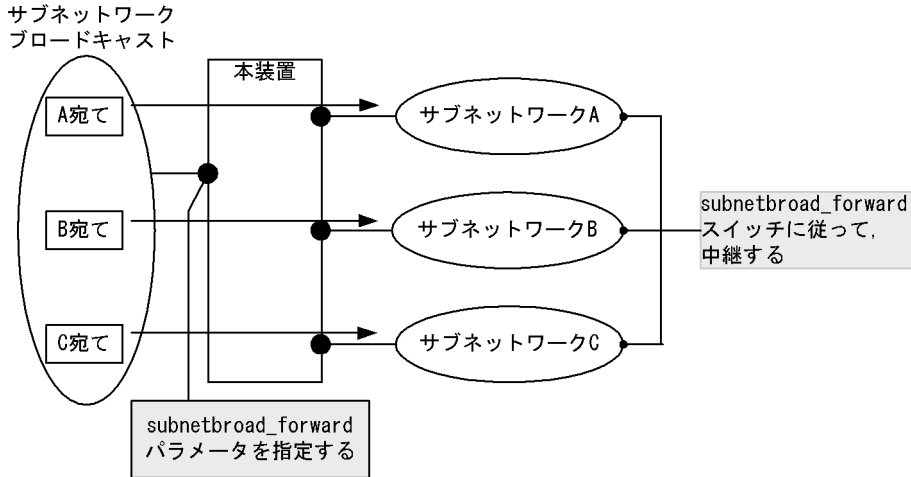
図 11-9　入力インタフェースで中継可否を決定する設定例

両スイッチを同時に使用することもできます。使用した場合には directbroad_forward スイッチが優先されます。両スイッチ併用設定例を「図 11-10　両スイッチ併用設定例」に示します。また，両スイッチを指定した場合の組み合わせを「表 11-7　両スイッチを指定した場合の組み合わせ」に示します。

図 11-10　両スイッチ併用設定例

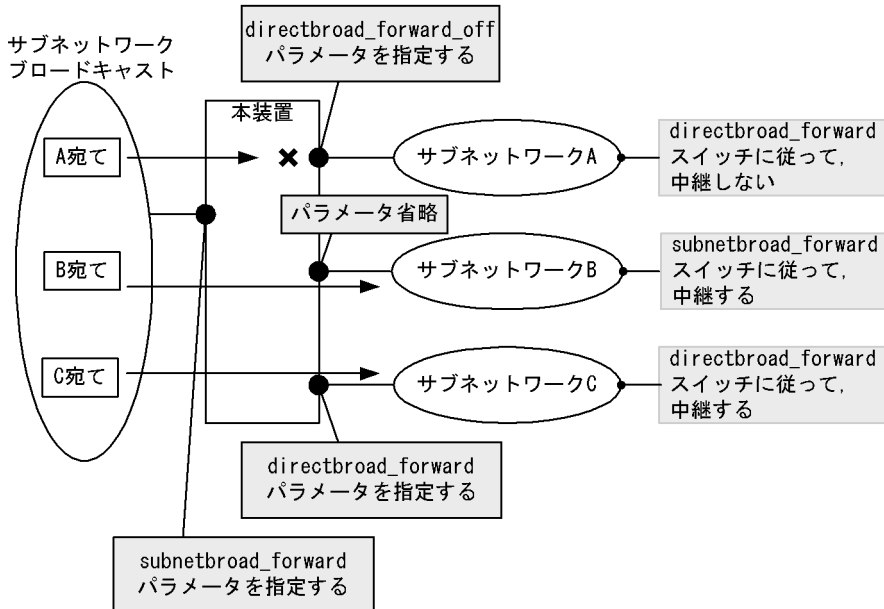



表 11-7　両スイッチを指定した場合の組み合わせ

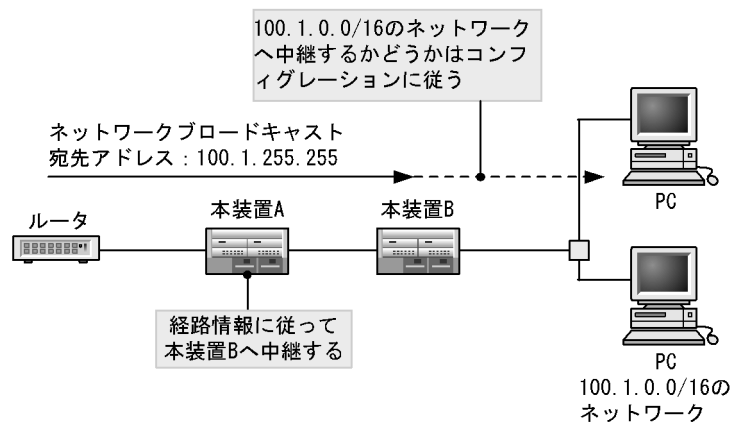
subnetbroad_forward スイッチ	directbroad_forward スイッチ		
	ON	OFF	指定なし
ON	○※	×※	○
OFF	○※	×※	×

subnetbroad_forward スイッチ	directbroad_forward スイッチ		
	ON	OFF	指定なし
指定なし	○	×	×

（凡例） ○：中継する ×：中継しない
注※ 両スイッチを併用している場合の優先度を次に示します。
directbroad_forward 指定 > subnetbroad_forward 指定

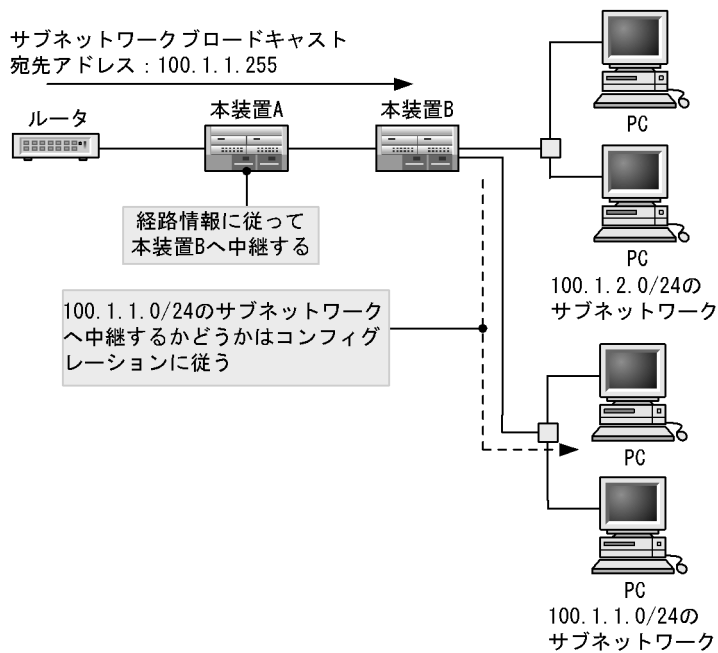
(1) ネットワークブロードキャスト

ネットワークブロードキャストとは，サブネットワーク化されていないネットワークに対するブロードキャストです。例えば，100.1.0.0/16 のネットワークに対して，100.1.255.255 を宛先とするネットワークブロードキャストの IP パケットが送信された場合，本装置が 100.1.0.0/16 のネットワークと直接接続しているときはコンフィグレーションのブロードキャスト中継スイッチの設定に従い，ネットワークブロードキャストの IP パケットを自装置配下へ中継するかどうかを判断します。ネットワークブロードキャストを次の図に示します。

図 11-11 ネットワークブロードキャスト

(2) サブネットワークブロードキャスト

サブネットワークブロードキャストとは，サブネットワーク化されたネットワークに対するブロードキャストです。

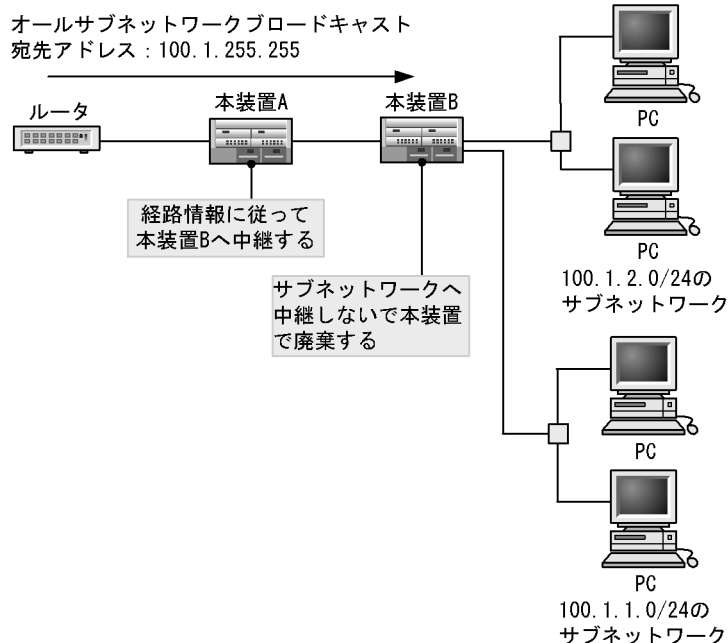
例えば，100.1.0.0/16 のネットワークをサブネットワーク化して，100.1.1.0/24，100.1.2.0/24 の二つのサブネットワークに分割して使用している場合に，100.1.1.255 を宛先とするサブネットワークブロードキャスト（サブネットワーク 100.1.1.0/24 へのブロードキャスト）の IP パケットが送信された場合，本装置が 100.1.1.0/24 のサブネットワークと直接接続しているときはコンフィグレーションのブロードキャスト中継スイッチの設定に従い，サブネットワークブロードキャストの IP パケットを自装置配下へ中継するかどうかを判断します。サブネットワークブロードキャストを次の図に示します。

図 11-12　サブネットワークブロードキャスト

(3)　オールサブネットワークブロードキャスト

オールサブネットワークブロードキャストとは，サブネットワーク化されたすべてのネットワークに対するブロードキャストです。

例えば，100.1.0.0/16 のネットワークをサブネットワーク化して，100.1.1.0/24 と 100.1.2.0/24 の二つのサブネットワークに分割して使用している場合に，100.1.255.255 を宛先とするオールサブネットワークブロードキャストの IP パケットが送信された場合，100.1.1.0/24 と 100.1.2.0/24 のサブネットワークを直接接続する本装置までは該当パケットが届きますが，本装置配下の 100.1.1.0/24 と 100.1.2.0/24 のサブネットワークへは中継しないで本装置で該当パケットを廃棄します。オールサブネットワークブロードキャストを次の図に示します。

図 11-13　オールサブネットワークブロードキャスト

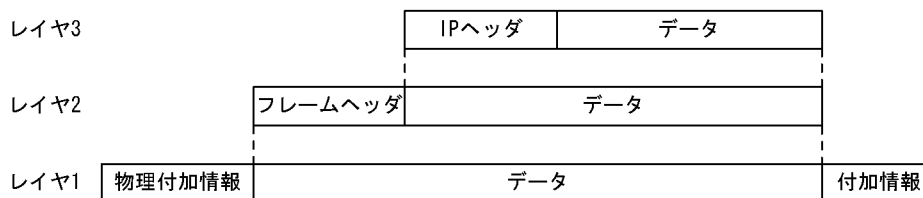
オールサブネットワークブロードキャスト
宛先アドレス：100.1.255.255
ルータ
本装置A
本装置B
経路情報に従って
本装置Bへ中継する
サブネットワークへ
中継しないで本装置
で廃棄する
PC
PC
100.1.2.0/24の
サブネットワーク
PC
PC
100.1.1.0/24の
サブネットワーク

11.5.3　MTU とフラグメント

IP パケットを中継するとき，最大転送単位（MTU：Maximum Transfer Unit）に従い，それ以上大きなパケットは分割して送信します。これを**フラグメント化**といいます。MTU のサイズに収まるパケットはハードウェア処理で中継しますが，分割して送信する場合はソフトウェア処理で中継するため中継パフォーマンスが低下しますので注意が必要です。

（1）最大フレーム長と MTU の決定

（a）インタフェースに対してポートが一つ存在する際の MTU 値の決定

ネットワーク内の中継装置を経由するレイヤ 3 パケット（IP パケット）は，回線を流れる物理フレームの中にカプセル化されています。カプセル化を次の図に示します。

図 11-14　カプセル化

物理フレームの最大長は，規格書の最大値を固定として持つもの，コンフィグレーションで定義するもの，さらにプロトコルでネゴシエーションするものがあり，物理種別やレイヤ 2 プロトコルによって MTU のサイズが決定します。フレームフォーマットおよび最大フレーム長については，「4　イーサネット」を参照してください。

コンフィグレーションで最大フレーム長または MTU サイズを指定できる場合については，マニュアル「コンフィグレーションコマンドレファレンス Vol.1」を参照してください。

(b) インタフェースに対してポートが複数存在する際の MTU 値の決定

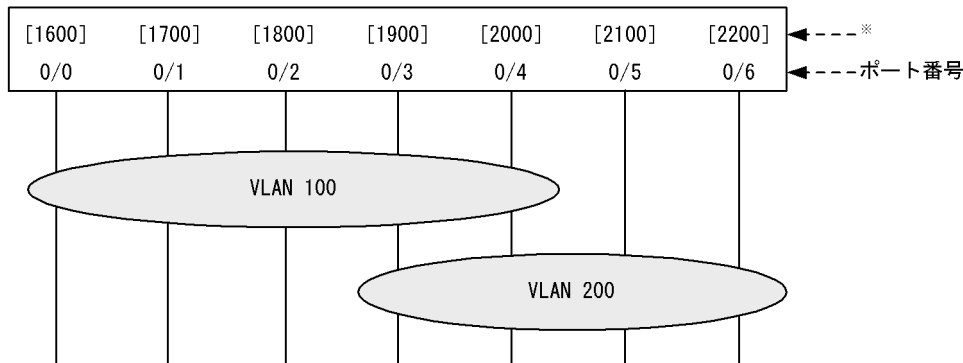
VLAN インタフェースやリンクアグリゲーションインタフェースのようにポートが複数存在するインタフェースの MTU 値の決定方法を次に示します。

● VLAN インタフェース

VLAN 情報の untagged-port サブコマンド，tagged-port サブコマンドで指定したポート内の Line 情報の jumbo_frame サブコマンドの最小値から 18byte※減算した値を MTU 値とします。また，IP 情報の mtu サブコマンドが設定されていた場合は mtu サブコマンドの値と untagged-port サブコマンド，または tagged-port サブコマンドで指定したポート内の jumbo_frame サブコマンドの値の最小値から 18byte 減算した値を比較し，小さい方を MTU 値として採用します。

注※

18byte の詳細は，「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。また，Line 情報の jumbo_frame サブコマンド未設定時に関しては，「コンフィグレーションコマンドレファレンス Vol.1　4. ライン情報」の line(Line 情報) を参照してください。

図 11-15　VLAN インタフェースの設定例

注※　Line 情報の jumbo_frame サブコマンドで設定した値より 18byte 減算した値です。

- IP 設定無しの場合

[MTU 決定値]

VLAN 100 の MTU 値・・・1600
VLAN 200 の MTU 値・・・1900

- IP 設定有りの場合

VLAN 100 に ip mtu 1000，VLAN 200 に ip mtu 3000 を定義したとき

[MTU 決定値]

VLAN 100 の MTU 値・・・1000
VLAN 200 の MTU 値・・・1900

● リンクアグリゲーションインタフェース

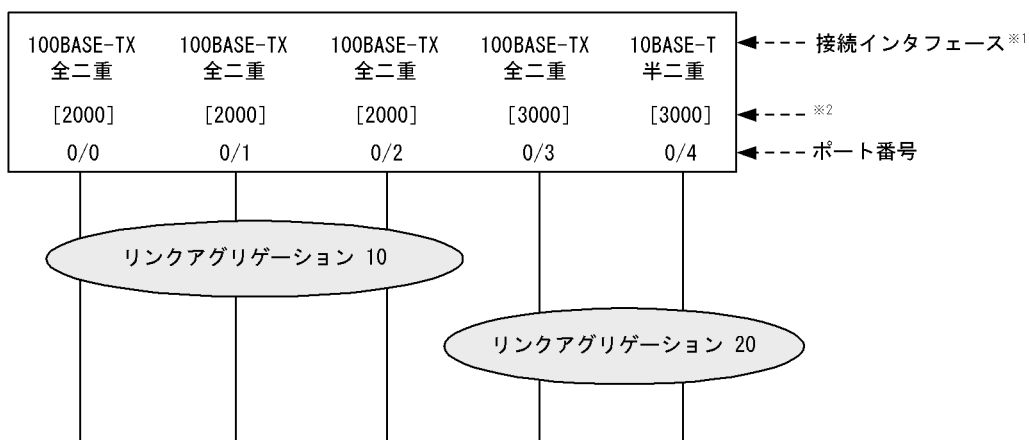
リンクアグリゲーション情報の aggregated-port サブコマンドで指定したポート内の Line 情報の jumbo_frame サブコマンドの最小値から 18byte※減算した値を MTU 値とします。また，IP 情報の mtu サブコマンドが設定されていた場合は，mtu サブコマンドの値と aggregated-port サブコマンドで指定したポート内の jumbo_frame サブコマンドの値の最小値から 18byte 減算した値を比較し，小さい方を MTU 値として採用します。

注※

18byte の詳細は，「4.3　MAC および LLC 副層制御」のフレームフォーマットを参照してくださ

い。また，Line 情報の jumbo_frame サブコマンド未設定時に関しては，「コンフィグレーションコマンドレファレンス Vol.1 4. ライン情報」の line(Line 情報) を参照してください。

図 11-16 リンクアグリゲーションインタフェースの設定例

注※ 1

接続インタフェースに関しては，「4.2 物理インタフェース」を参照してください。

注※ 2

Line 情報の jumbo_frame サブコマンドで設定した値より 18byte 減算した値です。

- IP 設定無しの場合

[MTU 決定値]

リンクアグリゲーション 10 の MTU 値・・・2000
リンクアグリゲーション 20 の MTU 値・・・1500

- IP 設定有りの場合

リンクアグリゲーション 10 に ip mtu 1000，リンクアグリゲーション 20 に ip mtu 3000 を定義したとき

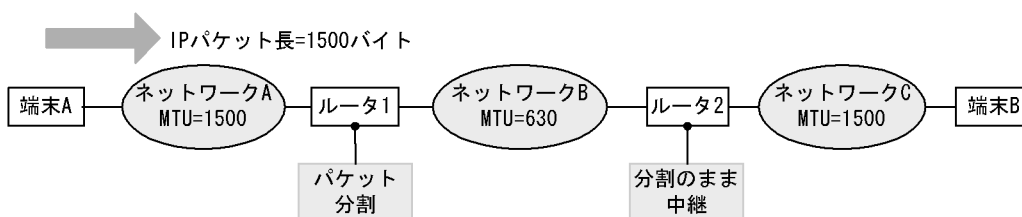
[MTU 決定値]

リンクアグリゲーション 10 の MTU 値・・・1000
リンクアグリゲーション 20 の MTU 値・・・1500

(2) MTU とフラグメント

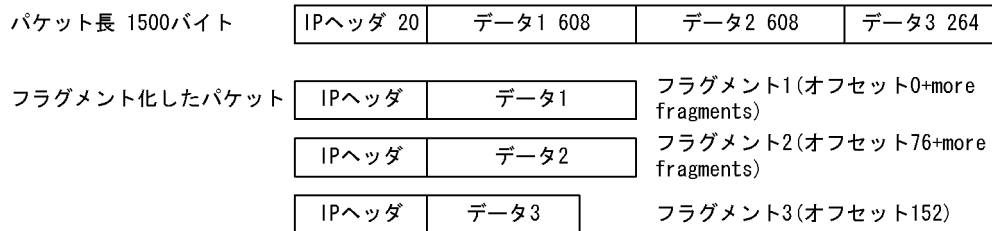
ネットワークの中には異なる MTU のサブネットワークがある可能性があります。サイズの大きな IP パケットを，小さな MTU を持つネットワークを通る場合，IP パケットを分割し中継します。

フラグメント化モデルを次の図に示します。ネットワーク A から送信したパケットをネットワーク B へ中継するとき，MTU が 1500 から 630 に短くなるためにフラグメント化します。

図 11-17 フラグメント化モデル

(3) フラグメントの生成

MTU を超える IP パケットは，IP ヘッダを除くデータ部分を 8 の倍数長でフラグメント化します。

ネットワーク B は MTU が 630 ですから，IP ヘッダ長を除くと 610 となり，610 での 8 の倍数長は 608 なので 608 バイトずつフラグメント化します。フラグメント化したパケットにはそれぞれ IP ヘッダを付加します。パケットのフラグメント化を次の図に示します。

図 11-18 パケットのフラグメント化

MTU に収まるようにフラグメント化した IP パケットは，フラグメント化したことを IP ヘッダ内のオフセットと more fragments ビットに書き込みます。また，同一の identification を設定して checksum を再計算します。オフセットは，先頭からのデータ長を 8 で割った値を設定します。

(4) フラグメントの再構成

フラグメント化された IP パケットは，終端で IP ヘッダ内の identification，オフセット，more fragments を基に再構成します。途中のルータは再構成を行いません。それは，終端までの中継で各フラグメントを独立して経路制御させることを前提としているため，仮に途中のルータがフラグメントを蓄積し再構成しようとした場合，そのルータを通過しなかったフラグメントがあると，蓄積していたフラグメントを破棄することになるためです。

11.5.4 包含サブネットの注意事項

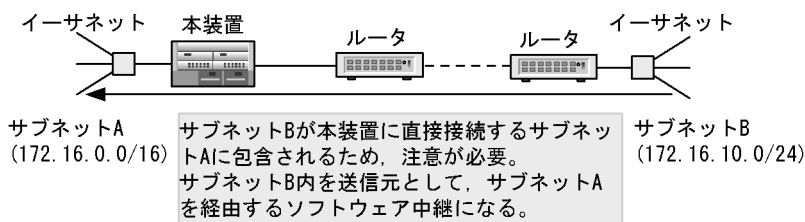
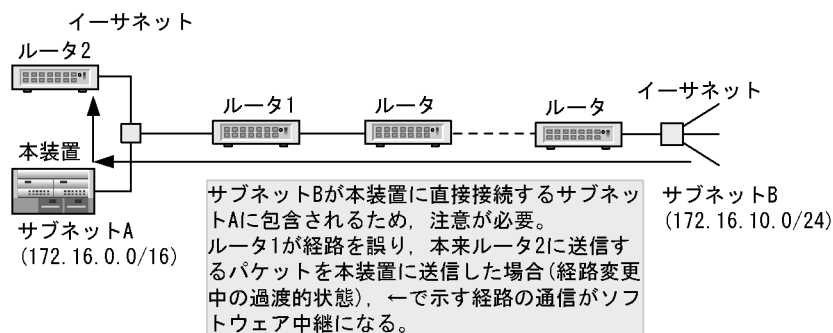
本装置に直接接続するサブネットアドレスに包含されるアドレスを，直接接続するサブネットの一つのインタフェース以外には割り当てることがないようにネットワーク全体のアドレスを設計してください（ポイント‐ポイント型回線の自装置側のアドレスには例外的に他サブネットに包含されるアドレスを付けることができます）。

このため，他サブネットを包含するサブネットを構成することはパケット中継の性能劣化の原因となりますが，これはこのマニュアルで説明しているルーティングプロトコルの経路集約を制限するものではありません。包含サブネットワークで注意する必要がある構成例を次に示します。

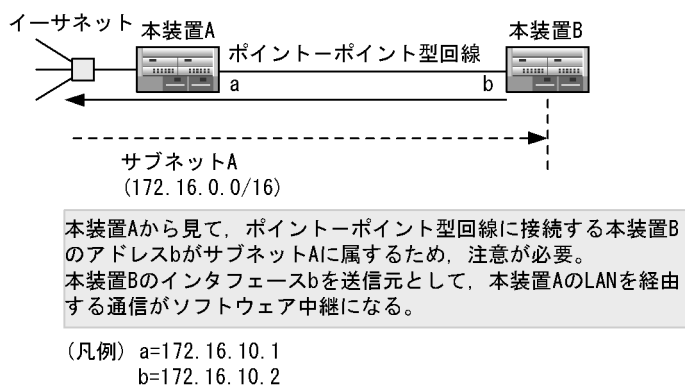
(1) あるサブネットが本装置に直接接続するサブネットに包含される場合の構成例

あるサブネットが本装置に直接接続するサブネットに包含される場合の構成例を次の図に示します。

図 11-19　包含サブネットワークの構成例 (あるサブネットが本装置に直接接続するサブネットに包含される場合)

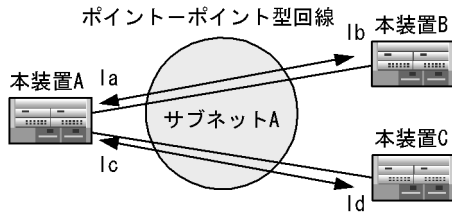
●構成例1

●構成例2

(2)　異なるインタフェースに接続する装置が同じサブネットに属する場合

異なるインタフェースに接続する装置が同じサブネットに属する場合の構成例を次の図に示します。

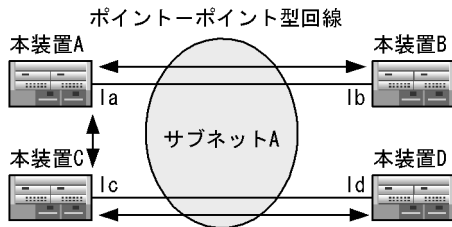
図 11-20　包含サブネットワークの構成例 (異なるインタフェースに接続する装置が同じサブネットに属する場合)

(3)　ポイント - ポイント型回線で同一サブネットアドレスが割り当てられた場合

ポイント - ポイント型回線で同一サブネットアドレスが割り当てられた場合の構成例を次の図に示します。

図 11-21　ポイント - ポイント型回線での同一サブネットアドレス割り当て構成例 1

●構成例1

本装置Aから見て，異なるインタフェースが同一サブネットに属しているが，ハードウェア中継になる。

（凡例）Ia=172.16.10.1
Ib=172.16.10.2
Ic=172.16.10.3
Id=172.16.10.4

●構成例2

アドレスIc，Idが本装置Aに直接接続するサブネットAに属するが，ハードウェア中継になる。
アドレスIa，Ibが本装置Cに直接接続するサブネットAに属するが，ハードウェア中継になる。

（凡例）Ia=172.16.10.1
Ib=172.16.10.2
Ic=172.16.10.3
Id=172.16.10.4

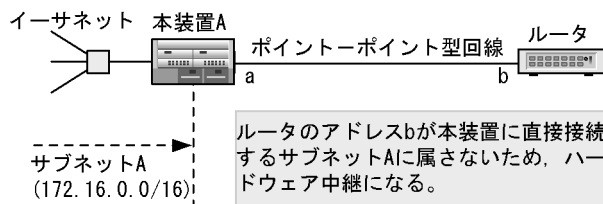
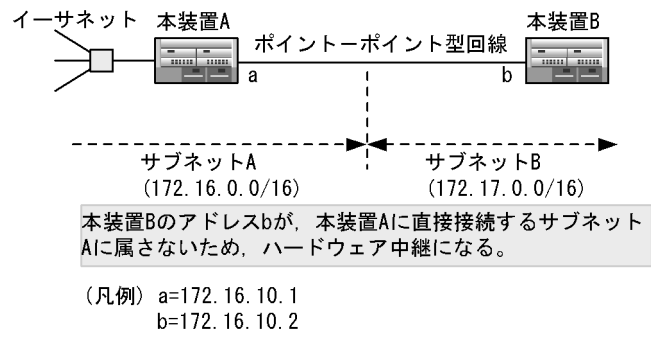
(4) 異なるインタフェースに接続する装置が異なるサブネットに属する場合

異なるインタフェースに接続する装置が異なるサブネットに属する場合の構成例を次の図に示します。

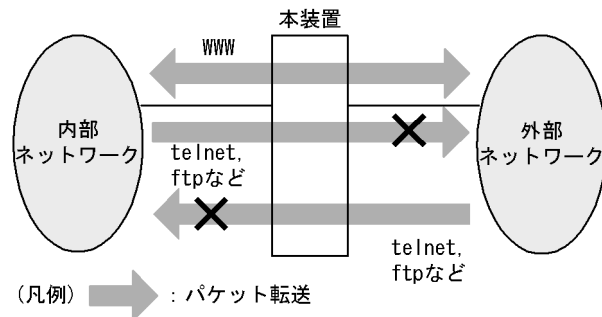
図 11-22　包含サブネットワークの構成例 (異なるインタフェースに接続する装置が異なるサブネットに属する場合)

●構成例1

（凡例）a=172.16.10.1
b=172.16.10.2

●構成例2

イーサネット
本装置A
ポイントーポイント型回線
本装置B
a
b
サブネットA
(172.16.0.0/16)
サブネットB
(172.17.0.0/16)
本装置Bのアドレスbが，本装置Aに直接接続するサブネットAに属さないため，ハードウェア中継になる。
(凡例) a=172.16.10.1
b=172.16.10.2

11.6 フィルタリング

フィルタリングは，受信したある特定のパケットを中継または廃棄する機能です。フィルタリングはネットワークのセキュリティを確保するために使用します。フィルタリングを使用すれば，例えば，内部ネットワークと外部ネットワーク間で WWW は中継するが，WWW 以外の telnet や ftp のパケットは廃棄したいなどの運用ができます。外部ネットワークからの不正なアクセスを防ぎ，また，内部ネットワークから外部ネットワークへ不要な情報の漏洩を防ぐことができます。フィルタリングを使用したネットワーク構成例を次に示します。

図 11-23　フィルタリングのネットワーク構成

11.6.1 フィルタリングの仕組み

フィルタリングする条件には，プロトコル番号，送信元 IP アドレス，宛先 IP アドレスなどのフロー検出条件があります。これらの条件を単一または複数指定してフィルタリングします。その検出条件と中継や廃棄という動作指定の組み合わせをフィルタエントリと呼びます。インタフェースの入力，出力毎にフィルタエントリを設定します。

フィルタリングの仕組みを次に示します。

1. 各インタフェースに設定したフィルタエントリを順番に検索します。
2. 一致したフィルタエントリが見つかった時点で検索を終了します。
3. 該当したパケットはフィルタエントリで設定した動作指定に従って，中継や廃棄等の動作が実行されます。

なお，一致したフィルタエントリが見つかった後は，フィルタエントリを検索しません。

すべてのフィルタエントリに一致しなかった場合は，そのパケットを中継します。

11.6.2 フロー検出条件

フロー検出条件を次の表に示します

表 11-8　フロー検出条件

ヘッダ種別	設定項目	項目設定
MAC	送信元 MAC アドレス※	MAC アドレスを単一指定，またはマスク指定できます。
	宛先 MAC アドレス※	MAC アドレスを単一指定，またはマスク指定できます。
	イーサネットタイプ※	IPv4，IPv6，IPX などのプロトコル種別を指定します。

ヘッダ種別	設定項目	項目設定
	ユニキャストフラッディングフレーム識別子※	フラッディングされたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出します。出力側だけ指定できます。
Tag-VLAN	VLAN ID ※	VLAN 番号
	ユーザ優先度	優先度情報
IP	IP ユーザデータ長	IP ユーザデータの上限値または下限値
	上位プロトコル	TCP，UDP などを示す番号
	送信元 IP アドレス	アドレスを単一指定，範囲指定，またはサブネット指定できます。
	宛先 IP アドレス	アドレスを単一指定，範囲指定，またはサブネット指定できます。
	DSCP	TOS フィールドの上位 6 ビット
	プレシデンス	TOS フィールドの上位 3 ビット
	フラグメント識別子	2 番目以降のフラグメントパケットを検出します。
TCP	送信元ポート番号	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	宛先ポート番号を単一指定，または範囲指定できます。
	ACK フラグ	ACK フラグが 1 のパケットを検出します。
	SYN フラグ	SYN フラグが 1 のパケットを検出します。
UDP	送信元ポート番号	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	宛先ポート番号を単一指定，または範囲指定できます。
ICMP	ICMP タイプ	Echo Request/Echo Reply/Destination Unreachable などを示す番号
	ICMP コード	Net Unreachable などの ICMP タイプに対する詳細コードを示す番号
IGMP	IGMP タイプ	Membership Query などを示す番号

注※

出力側のインタフェースで，送信元 MAC アドレス，宛先 MAC アドレス，イーサネットタイプ，および VLAN ID で IPv4，IPv6 中継パケットを検出することはできません。

本装置は，イーサネットタイプとしてイーサネット V2 形式と，IEEE802.3 の SNAP/RFC1042 形式のイーサネットフレームのイーサネットタイプを検出できます。イーサネットタイプの位置を次の図に示します。

図 11-24　イーサネットタイプの位置

イーサネットV2形式

宛先MAC アドレス	送信元MAC アドレス	イーサネット タイプ	データ	FCS

IEEE802.3 SNAP/RFC1042形式

宛先MAC アドレス	送信元MAC アドレス	長さ	DSAP= 0xAA	SSAP= 0xAA	制御= 0x03	SNAP OUI =0x000000	イーサネット タイプ	データ	FCS

ユニキャストフラッディングフレーム識別子 (unicast_flood) は，本装置がフラッディングしたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出するための条件です。フラッディングとは，フレームを受信した物理ポートを除く同一 VLAN 内の全ポートへ，フレームを転送する動作で

す。

11.6.3　フィルタリングの運用について

フィルタリングでは，フロー検出条件モードおよびフロー検出条件オプションで運用方法を選択できます。

(1)　フロー検出条件モード

フロー検出条件モードでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法はQoS 制御も同じ運用方法となります。

表 11-9　フロー検出条件モードで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件モードの指定方法
1	きめ細かいフロー検出条件を指定する	MAC，IP ヘッダなどを検出条件としてパケット検出が可能。	フロー検出条件モードの指定なし
2	パケット中継性能を劣化させない	<Portlist> 指定では，L2 スイッチ中継を対象とし，<Interface Name> 指定では，IPv4，IPv6 中継パケットを対象としたパケット検出が可能。	フロー検出条件モード 1 (retrieval_mode_1) を指定

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 11-10　フロー検出条件モードと対応可能 PSU，BSU の関係

フロー検出条件モード	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2
フロー検出条件モード 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a)　フロー検出条件モード 1

パケット中継性能を劣化させることなく，フィルタリング機能を使用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件モード 1 を指定します。

フロー検出条件モード 1 を有効とするには，指定 PSU に「表 11-10　フロー検出条件モードと対応可能 PSU，BSU の関係」で示す対応可能 PSU を実装してください。フロー検出条件モード 1 をサポートしていない PSU に対してフロー検出条件モード 1 を設定した場合，フローフィルタ機能，フロー QoS 機能は動作しません。

フロー検出条件モード 1 指定時，設定した入出力インタフェースごと (<Portlist> 指定，または <Interface Name> 指定) に指定可能なフロー検出条件を「表 11-11　フロー検出条件モード 1 時のフロー検出条件」に示します。

なお，QoS 制御もフロー検出条件モード 1 で動作します。フロー検出条件モード 1 指定時，QoS 制御で指

定可能なフロー検出条件は，「解説書 Vol.2　1.3.1 フロー検出機能の運用について」を参照してください。

表 11-11　フロー検出条件モード 1 時のフロー検出条件

ヘッダ種別	設定項目	<Portlist> 指定	<Interface Name> 指定
MAC	送信元 MAC アドレス	○	-
	宛先 MAC アドレス	○	-
	イーサネットタイプ	○	-
	ユニキャストフラッディングフレーム識別子	○※	-
Tag-VLAN	VLAN ID	○	-
	ユーザ優先度	○	○
IP	IP ユーザデータ長	-	○
	上位プロトコル	-	○
	送信元 IP アドレス	-	○
	宛先 IP アドレス	-	○
	DSCP	○	○
	プレシデンス	○	○
	フラグメント識別子	-	○
TCP	送信元ポート番号	-	○
	宛先ポート番号	-	○
	ACK フラグ	-	○
	SYN フラグ	-	○
UDP	送信元ポート番号	-	○
	宛先ポート番号	-	○
ICMP	ICMP タイプ	-	○
	ICMP コード	-	○
IGMP	IGMP タイプ	-	○

(凡例)　○：指定可　-：指定不可
注※　出力側だけ指定可能です。

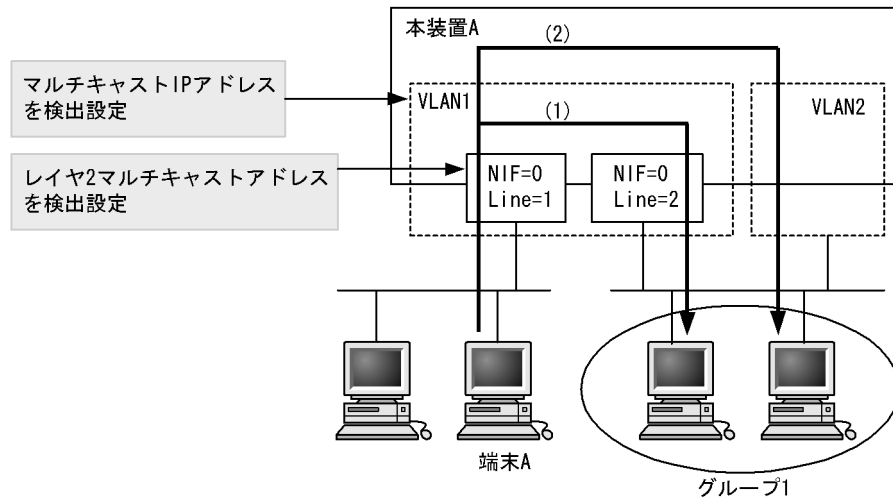
次にフロー検出条件モード 1 を使用した場合の <Portlist> 指定，<Interface Name> 指定ごとの検出可能なパケットを示します。

表 11-12　検出可能パケット種別一覧

フロー指定方法	パケット種別
<Portlist> 指定	レイヤ 2 スイッチ中継パケット※
<Interface Name> 指定	IPv4，IPv6 中継パケット※

注※
宛先 MAC アドレスがレイヤ 2 マルチキャストアドレス，かつ宛先 IP アドレスがマルチキャスト IP アドレスのパケットは，本装置でレイヤ 2 スイッチ中継および IPv4，IPv6 中継の両方を実施します (次に示す図の (1)，(2))。したがって，コンフィグレーションコマンド flow filter で，(1) のレイヤ 2 スイッチ中継パケットをフロー検出する場合は，<Portlist> 指定で宛先 MAC アドレス検出条件にレイヤ 2 マルチキャストアドレスを指定して，(2) の

IPv4 中継パケットをフィルタリングする場合は <Interface Name> 指定で，宛先 IPv4 アドレス検出条件にマルチキャスト IP アドレスを指定してください。

図 11-25　マルチキャストパケット中継例

(2) フロー検出条件オプション

フロー検出条件オプションでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法は QoS 制御も同じ運用方法となります。

表 11-13　フロー検出条件オプションで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件オプションの指定方法
1	中継パケットでフロー検出する	中継パケットでだけフロー検出可能	フロー検出条件オプションの指定なし
2	中継パケットおよび本装置宛パケット※でフロー検出したい	中継パケットおよび本装置宛パケット※でフロー検出可能	フロー検出条件オプション 1 (retrieval_option_1) を指定

注※

フロー検出条件オプション 1 指定時にフロー検出対象に加わる本装置宛パケットは，次に示すパケットです。したがって，フロー検出条件オプション 1 を指定しない場合，次に示す本装置宛パケットはフロー検出対象外です。

- 宛先 MAC アドレスがブロードキャストアドレスであるパケット
- 宛先 MAC アドレスがマルチキャスト MAC アドレスまたは自 MAC アドレスである非 IP パケット

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 11-14　フロー検出条件オプションと対応可能 PSU，BSU の関係

フロー検出条件オプション	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

フロー検出条件オプション	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
フロー検出条件オプション 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a)　フロー検出条件オプション 1

本装置宛パケット（「表 11-13　フロー検出条件オプションで選択できる運用方法」の注参照）でもフロー検出機能を運用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件オプション 1 を指定します。フロー検出条件オプション 1 を使用する場合は，対象 PSU，対象 BSU に「表 11-14　フロー検出条件オプションと対応可能 PSU，BSU の関係」で示す対応可能 PSU，BSU を実装してください。なお，QoS 制御もフロー検出条件オプション 1 で動作します。また，フロー検出条件オプション 1 の指定は，フロー検出条件モードと同時に設定できます。

注

EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出するコンフィグレーション flow filter の設定は，次のインタフェースまたは物理ポートに指定してください。

- Tag-VLAN 連携回線の untagged の論理インタフェース
- VLAN 回線の untagged ポートが属する VLAN インタフェース

11.6.4　フロー検出とパケット中継方式との対応

パケット中継方式によってフロー検出可能なパケットが異なります。パケット中継方式との対応を，「表 11-15　パケット中継方式との対応」に示します。

表 11-15　パケット中継方式との対応

フロー検出		レイヤ 2 スイッチ中継		IPv4 中継	
		受信側	送信側	受信側	送信側
MAC ヘッダ	送信元 MAC アドレス	○	○	○	○※ 1
	宛先 MAC アドレス	○	○	○	○※ 1
	イーサネットタイプ	○	○	○	-
Tag-VLAN ヘッダ	ユーザ優先度	○	○※ 2	○	○※ 3
	VLAN ID	○	○	○	○※ 4
IP ヘッダ※ 5		○	○	○	○
レイヤ 4 ヘッダ (TCP/UDP など) ※ 5		○	○	○※ 6	○※ 6

(凡例)　○：サポート　　-：未サポート

注※ 1

特定の MAC アドレスのフロー検出は未サポートです。すべての MAC アドレスをフロー検出すること（コンフィグレーションコマンド flow filter での MAC アドレスに any と指定）ができます。

注※ 2

レイヤ 2 スイッチ中継で，送信側でのユーザ優先度で検出を指定したときは，次のようになります。

- 受信側で VLAN-Tag 無しフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

- 受信側で VLAN-Tag 付きフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，受信時のユーザ優先度で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※ 3
IPv4 中継で，送信側でユーザ優先度のフロー検出を指定したときは，次のようになります。
- 受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
- 受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※ 4
インタフェース名指定で，Tag-VLAN 連携回線の場合，VLAN ID をフロー検出条件として指定する必要はありません。

注※ 5
Tag-VLAN ヘッダが 2 個までの場合です。3 個以上の場合は未サポートです。

注※ 6
2 番目以降のフラグメントパケットを 4 層 (TCP，UDP，ICMP，IGMP) のフロー検出条件でフィルタリングを実施した場合，2 番目以降のフラグメントパケットはレイヤ 4 ヘッダがパケット内にないため，同じフロー検出条件で検出できません。フラグメントパケットを含めたフィルタリングを実施する場合は，フロー検出条件に 3 層ヘッダ条件を指定するようにしてください。

11.6.5 フィルタリング使用時の注意事項

(1) フラグメントパケットをフロー検出する場合の注意事項

2 番目以降のフラグメントパケットを 4 層 (TCP,UDP,ICMP,IGMP) のフロー検出条件でフィルタリングを実施した場合，2 番目以降のフラグメントパケットはレイヤ 4 ヘッダがパケット内にないため，同じフロー検出条件で検出できません。フラグメントパケットを含めたフィルタリングを実施する場合は，フロー検出条件に 3 層ヘッダ条件を指定するようにしてください。

なお，先頭フラグメントパケットを中継した場合，2 番目以降のフラグメントパケットを常に中継します。

(2) レイヤ 2 スイッチ中継での IPv4 オプション付きパケットをフロー検出する場合の注意事項

レイヤ 2 スイッチ中継で，IPv4 オプション付きパケットを受信し，フロー検出条件としてポート番号などのレイヤ 4 ヘッダ検出条件を設定している場合：

1. パケットのレイヤ 4 ヘッダが見えるとき (次の表を参照してください)
   ハードウェア処理によってフィルタリングを実行します。
2. パケットのレイヤ 4 ヘッダが見えないとき (次の表を参照してください)
   フィルタリングで指定した動作を行わず，受信パケットを中継します。

表 11-16 受信側でのレイヤ 4 ヘッダ判別可否パターン

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP※1 ICMP/IGMP※2	TCP CODEBIT
IPv4 オプションなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv4 オプションあり (8byte 以下)	POS【**SB-7800S**】		○	×
	Ethernet V2	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
	IEEE802.3	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
IPv4 オプションあり (9byte 以上)	POS【**SB-7800S**】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○：該当フィールドの検出可 ×：該当フィールドの検出不可
注※ 1 ：送信元ポート番号 , 宛先ポート番号
注※ 2 ：Type,Code

表 11-17 送信側でのレイヤ 4 ヘッダ判別可否パターン

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
IPv4 オプションなし	POS【**SB-7800S**】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv4 オプションあり (8byte 以下)	POS【**SB-7800S**】		○	×
	Ethernet V2	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
	IEEE802.3	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
IPv4 オプションあり (9byte 以上)	POS【SB-7800S】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○：該当フィールドの検出可　×：該当フィールドの検出不可
注※ 1　：送信元ポート番号 , 宛先ポート番号
注※ 2　：Type,Code

(3) プライベート VLAN 使用時の注意事項

プライベート VLAN 機能を使用している VLAN に対するフィルタリング機能は，該当 VLAN の物理ポート (<Portlist> 指定) に対する設定だけサポートしています。該当 VLAN のインタフェース (<Interface Name> 指定) に対する設定は未サポートです。

(4) show filter-flow 運用コマンドのフローフィルタ統計情報の表示について

1. 下記条件を満たすコンフィグレーション flow filter を指定した物理ポートまたはインタフェースが，show vlan コマンドでの Port Information の表示において Blocking 状態の場合，廃棄したパケットのフローフィルタ統計情報は採取されません。
   - 条件 1
     フロー検出条件オプション 1 を指定
   - 条件 2
     コンフィグレーション flow filter で EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出し，廃棄動作指定を設定
2. フロー検出条件オプション 1 の指定時， 1 物理ポートだけ指定した VLAN 回線で，宛先 MAC アドレスが MAC ブロードキャストのパケットをフロー検出して forward 動作指定を指定した場合，フローフィルタ統計情報は採取されません。

11.6.6 FDB のスタティックエントリ登録機能との併用時の動作

MAC アドレスをフローの検出条件としてパケットの廃棄が可能となる機能として，フィルタリング機能と FDB のスタティックエントリ登録機能の二つがあります。次の表にフィルタリング機能と FDB のスタティックエントリ登録機能とを併用した場合のパケットの廃棄動作について示します。

表 11-18　FDB のスタティックエントリ登録機能との併用時のパケット廃棄動作

フィルタリング機能の動作指定	FDB のスタティックエントリ機能の動作指定	パケットの廃棄動作
中継	中継	-(中継します)
	廃棄	FDB のスタティックエントリ登録機能によってパケットを廃棄します
廃棄	中継	フィルタリング機能によってパケットを廃棄します
	廃棄	フィルタリング機能によってパケットを廃棄します

11.7　ロードバランス

11.7.1　ロードバランス概説

ロードバランスは，マルチパス接続（宛先ネットワークアドレスに対し複数の経路を構築）によって，IP レイヤのルーティング制御で，増大するトラフィックの負荷を分散する機能です。高帯域の回線にアップグレードしないで，既存の回線を集合して高帯域を供給します。

ここで説明するのはレイヤ 3 で実現するロードバランスです。

マルチパスを使用した負荷分散を「図 11-26　マルチパスを使用した負荷分散 (隣接ルータが単一の場合)」および「図 11-27　マルチパスを使用した負荷分散 (隣接ルータが複数の場合)」に示します。この図では四つのパスを利用して，ネットワーク A からネットワーク B 内のサーバ宛てのパケットをハードウェア処理で高速に中継します。

図 11-26　マルチパスを使用した負荷分散 (隣接ルータが単一の場合)

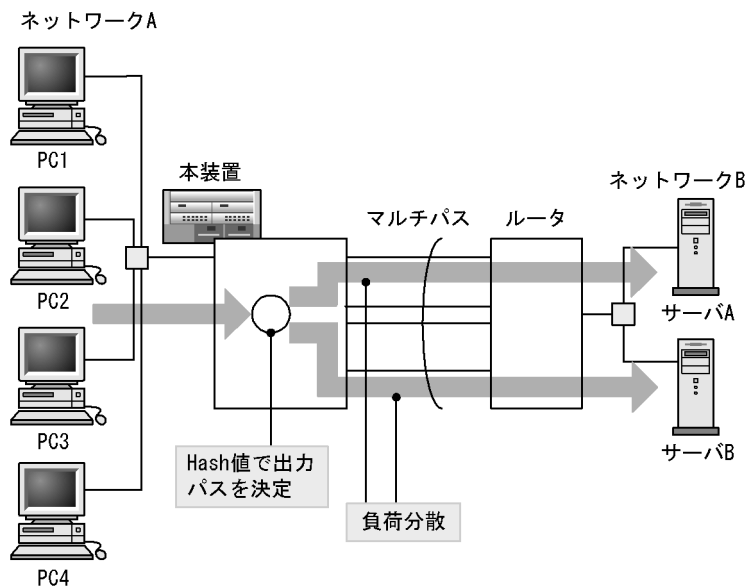
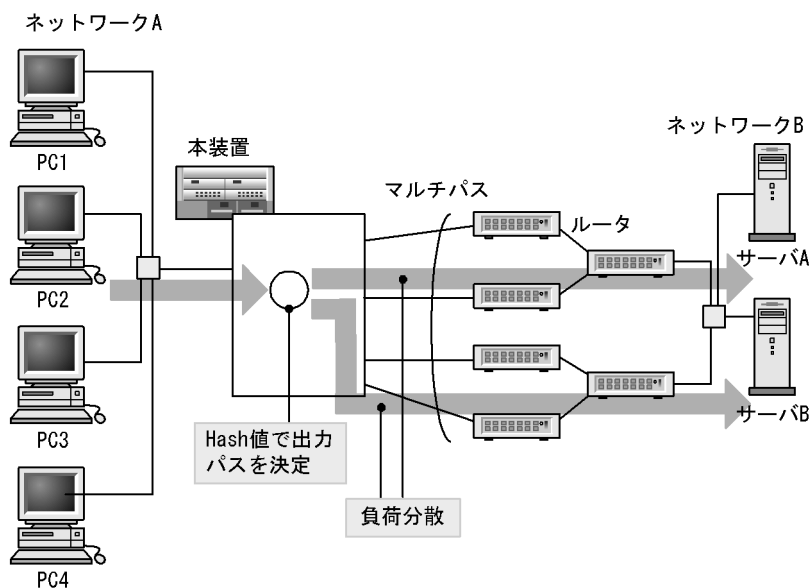



図 11-27　マルチパスを使用した負荷分散 (隣接ルータが複数の場合)

11.7.2　ロードバランス仕様

本装置で実装するマルチパスの仕様を「表 11-19　マルチパス仕様」に，ロードバランスの仕様を「表 11-20　ロードバランス仕様」に示します。デフォルトのコンフィグレーションでは，マルチパスは無効になっているので，使用するときはマルチパスの最大パス数と各ルーティングプロトコルでのマルチパス生成を指定する必要があります。

表 11-19　マルチパス仕様

項目	仕様	備考
一宛先ネットワークに対するマルチパス数	2 ～ 16 パス	冗長構成の場合，選択するマルチパス数はコンフィグレーションで指定した数になります。
コンフィグレーションのマルチパス数指定	1 ～ 16 1 を指定したときはマルチパスを生成しません。	装置単位で指定します。
マルチパスで生成できるルーティングプロトコル	• スタティックルーティング (「12.3.1　スタティックルーティング」参照) • OSPF(「12.5.2　経路選択アルゴリズム」参照) • BGP4(「13.3.7　BGP4 マルチパス」参照) • IS-IS(「14.2.3　経路選択アルゴリズム」参照)	コンフィグレーションで各ルーティングプロトコルのマルチパス生成を指定する必要があります。
接続構成	回線種別およびインタフェース種別に関係なく使用できます。また，混在もできます。	-

(凡例)　- : 該当しない

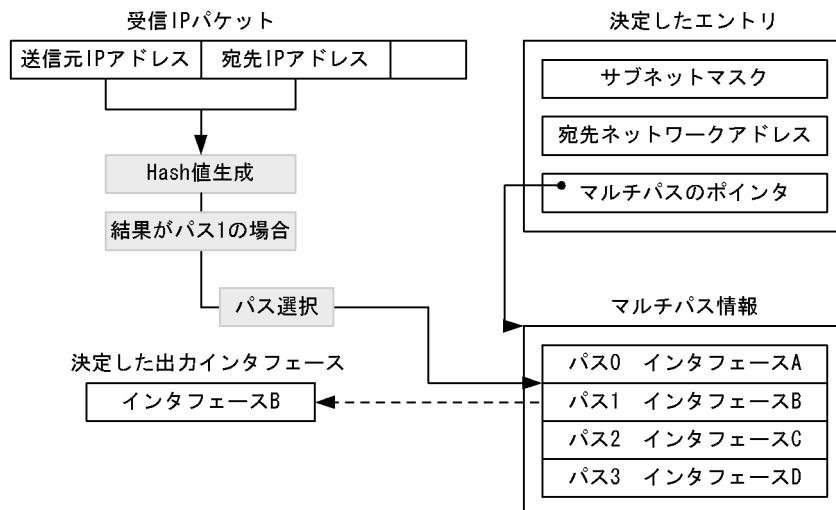
表 11-20 ロードバランス仕様

項目	仕様	備考
マルチパスの振り分け方法	宛先 IP アドレスと送信元 IP アドレスから 16 パスに振り分ける値 (hash 値) を算出し，決定した出力パスに振り分けます。宛先 IP アドレスと送信元 IP アドレスが同一のパケットは，同一出力パスを選択します。これによって，送信の順序性を保証します。	-
Hash 値	256 通り 宛先 IP アドレスと送信元 IP アドレスから算出します。	-
ルーティングテーブル内のマルチパス情報	ルーティングテーブルに設定する各出力インタフェースの hash の割り当て比率は，ほぼ均等になります。	「11.7.4 ロードバランス使用時の注意事項」の 1 および 2 を参照
各パスの重み付け	できません。	「11.7.4 ロードバランス使用時の注意事項」の 1 を参照
出力帯域を超えたパケットの処理	別のパスに振り分けません。継続して帯域を超えた場合は，装置内で保持しますが，保持しきれない場合はパケットを廃棄します。	「11.7.4 ロードバランス使用時の注意事項」の 4 を参照

(凡例) - : 該当しない

11.7.3 出力インタフェースの決定

ルーティングテーブルの検索で，宛先 IP アドレスに該当するエントリが決定すると，次に出力インタフェースを決定します。出力インタフェースは，受信した IP パケットの送信元 IP アドレス (Source IP Address) と宛先 IP アドレス (Destination IP Address) から Hash 値を生成し，それによってマルチパスの候補の一つを選択して決定します。出力インタフェースの決定を次の図に示します。

図 11-28 出力インタフェースの決定

(1) Hash 値の計算方法

次に，Hash 値の計算方法を示します。

Hash 値 $H[2^{7-0}]$($H[2^7]$ は 2^7 ビット，$H[2^0]$ は 2^0 ビット，$H[2^{7-0}]$ は 2^0 から 2^7 までのビット列を示す）は，8 ビットで生成します。

送信元 IP アドレスを $S[2^{31-0}]$，宛先 IP アドレスを $D[2^{31-0}]$ とした場合，Hash 値 $H[2^{7-0}]$ の計算式は，次のとおりです。

$H[2^{7-0}]$ は，送信元 IP アドレスと宛先 IP アドレスの値を，8 ビットごとに加算した結果の下位 8 ビットをビット逆順にした値です。

$$H'[2^{7-0}] = S[2^{31-24}] + S[2^{23-16}] + S[2^{15-8}] + S[2^{7-0}] + D[2^{31-24}] + D[2^{23-16}] + D[2^{15-8}] + D[2^{7-0}]$$ （桁上げは無視）

$$H[2^{7-0}] = H'[2^{0-7}]$$ （ビットを逆順）

Hash 値計算方法を次の図に示します。

図 11-29　Hash 値計算方法

$S[2^{31-0}]$=192.168.1.1　$D[2^{31-0}]$=192.168.5.2

$S[2^{31-24}]$	$S[2^{23-16}]$	$S[2^{15-8}]$	$S[2^{7-0}]$
192	168	1	1

$D[2^{31-24}]$	$D[2^{23-16}]$	$D[2^{15-8}]$	$D[2^{7-0}]$
192	168	5	2

8ビットごとに加算（桁上げ無視）

$H'[2^{7-0}]$=0xD9

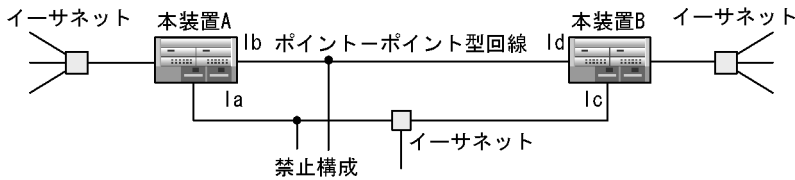
ビットを逆順にして　$H[2^{7-0}] = H'[2^{0-7}]$ = 0x9B = 155

選択パス = Hash値 × 有効パス数 ÷ 256 （小数点以下切り捨て）

= 155 × 4 ÷ 256 = 2 （有効パス数を4にした場合）

11.7.4　ロードバランス使用時の注意事項

1. Hash 値によって，一意に 16 パスの内 1 パスを選択するため，宛先ネットワークに対するそれぞれのパスのパケット分配比率は必ずしも均等になりません。
2. 各パスに対して重み付けをしないため，回線速度が異なる場合は速度に比例して分配しません。ただし，回線速度の速い回線に重み付けをするには，イーサネット回線の場合はマルチホーム接続によってできますが，障害の発生などを考慮し，冗長構成とする必要があります。
3. Hash 値によって選択した該当パスの出力帯域を超えて継続的にパケットを送出しようとした場合，パケット廃棄が発生します。別のパスには振り分けません。
4. マルチパスに Null インタフェースを含められません。
5. 2 台のルータ間をポイント - ポイント型回線でマルチパス接続をする場合，次の図に示す注意が必要です。

図 11-30 ポイント - ポイント型回線接続での制限

6. 本装置から自発送信する場合は , 送信元 IP アドレスを 0.0.0.0 として Hash 値を算出します。
7. traceroute コマンドによって，ロードバランスで使用する選択パスを確認する場合は次の注意が必要です。
   - traceroute コマンドを受信した回線の IP アドレスを送信元 IP アドレスとして，応答を返しますが，その回線を使用して応答を返すとは限りません。
   - traceroute コマンドを受信した回線がマルチホーム定義の場合，隣接装置がどのサブネットで送信したのか判断できないので，マルチホーム内の 1 アドレスを送信元 IP アドレスとして応答します。

11.8 Null インタフェース

Null インタフェースは，物理回線に依存しないパケット廃棄用の仮想的なインタフェースで，特定フローの出力先を Null インタフェースに向けることでパケットを廃棄する機能を提供します。

Null インタフェースは常に UP 状態にあり，トラフィックを中継または受信しません。廃棄したパケットに対して，送信元に ICMP(Unreachable) によるパケット廃棄の通知も行いません。また，マルチキャストパケットについては Null インタフェース上での廃棄は行いません。

Null インタフェースを使用して，本装置を経由する特定のネットワーク宛て，または特定の端末宛ての通信を制限できます。次の図では，本装置を経由するネットワーク B 宛ての通信をすべて Null インタフェースに向けて，ネットワーク B 宛てのパケットを廃棄することを示しています。

図 11-31 Null インタフェースネットワーク構成

この機能はスタティックルーティングの一部として位置づけられます。このため，Null インタフェースでパケット廃棄を行う場合，出力先が Null インタフェースになるスタティック経路情報を設定する必要があります。

経路検索時，Null インタフェース宛てと判断された (Null 宛てのスタティック経路情報に基づいてルーティングする) パケットは中継しないで本装置内で廃棄します。

スタティックルーティングおよび経路制御についての詳細は「12　RIP ／ OSPF」～「13　BGP4【OP-BGP】」を参照してください。

本装置では，インタフェース単位に複数の条件設定によってパケット廃棄ができるようにするフィルタリング機能も提供していますが，Null インタフェースは特定の宛先フローだけをスタティック経路として設定するだけで，装置で一括してパケット廃棄を行えるメリットがあります。

Null インタフェースとフィルタリング機能使用時のパケットの廃棄部位を次の表に示します。

表 11-21 Null インタフェースとフィルタリング機能使用時のパケットの廃棄部位

経路情報	フィルタリング設定		動作	廃棄部位
	入力側	出力側		
Null 宛て	中継	中継	廃棄	Null インタフェース
		廃棄	廃棄	
	廃棄	中継	廃棄	フィルタリング (入力側)
		廃棄	廃棄	

経路情報	フィルタリング設定		動作	廃棄部位
	入力側	出力側		
他経路宛て (Null 以外)	中継	中継	中継	-
		廃棄	廃棄	フィルタリング (出力側)
	廃棄	中継	廃棄	フィルタリング (入力側)
		廃棄	廃棄	

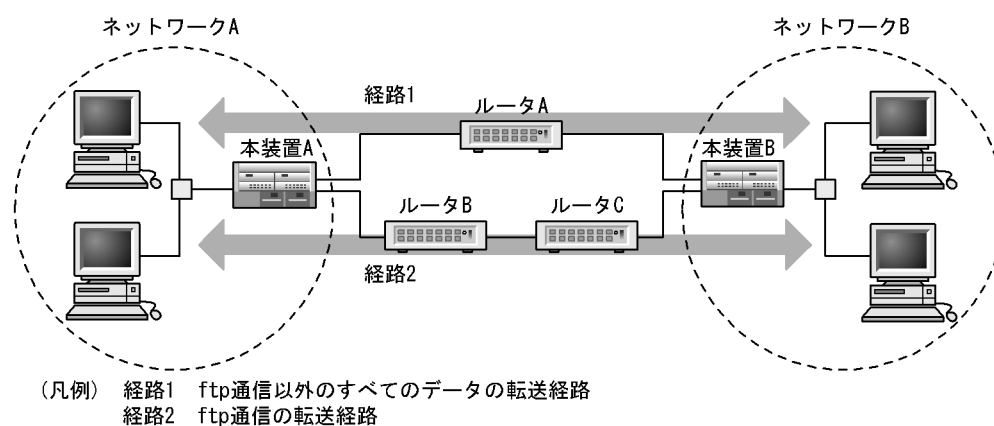
(凡例) - : 該当しない

11.9 ポリシールーティング

ポリシールーティングとは，ルーティングプロトコルで登録された経路情報に従わないで，ユーザが設定したポリシーをベースにして特定の経路にパケットを転送するルーティング方法です。

11.9.1 ポリシールーティング機能

次の図に示すネットワーク構成の場合，本装置 A は経路情報に従うとネットワーク A からネットワーク B 宛てのパケットは最短経路の経路 1 を使って中継されます。ここで，ポリシールーティング機能を使用してネットワーク A からネットワーク B 宛ての ftp 通信は経路 2 を使うように設定すると，経路 1 と経路 2 の負荷を分散できます。

図 11-32 ポリシールーティング

このように，ポリシールーティング機能は，ルーティングプロトコルでダイナミックに登録された経路情報に関係なく，ユーザのポリシーによってネットワークの経路を設定できます。

11.9.2 ポリシールーティング制御

本装置のポリシールーティングは，フィルタリング機能と組み合わせて使用します。ユーザが設定するポリシーはコンフィグレーションでフィルタエントリの Inbound 側フロー検出条件に一致したパケットを転送する経路情報として設定します。

経路情報は，コンフィグレーションの**ポリシールーティングリスト情報**で設定します。ポリシールーティングリスト情報は，256 個まで設定でき，単一または複数のポリシールーティングリスト情報をグループ化して**ポリシールーティンググループ情報**を定義します。

ポリシールーティンググループ情報に複数のポリシールーティングリスト情報を設定した場合，該当するポリシールーティングリスト情報をポリシールーティンググループ情報に設定した順番がパケットを転送する時に使用されるポリシールーティングリスト情報の優先順位になります。現在使用されているポリシールーティングリスト情報に設定された経路が障害などで転送できなくなった場合，同一のポリシールーティンググループ情報に設定された，次に優先度の高いポリシールーティングリスト情報に設定されている経路情報を使用してパケットを転送します。

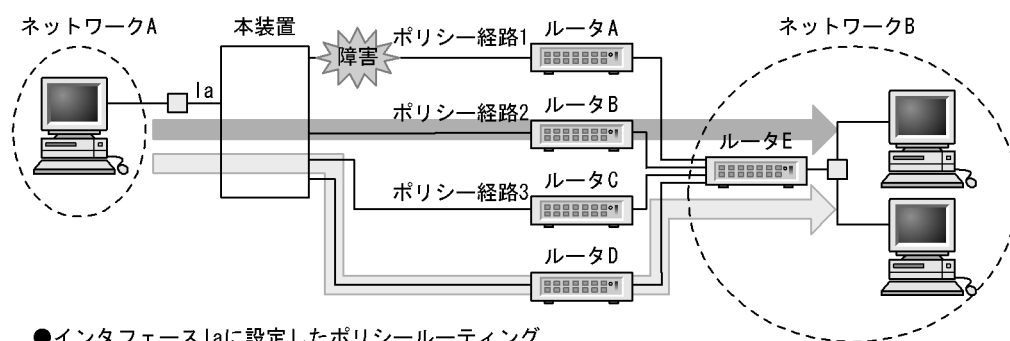
ポリシールーティングは，受信したパケットがフィルタエントリの Inbound 側フロー検出条件に一致し，フィルタエントリにポリシールーティンググループ情報が設定されている場合に行われます。受信側のフィルタエントリの Inbound 側フロー検出条件に一致しない場合，またはフロー検出条件の一致したフィルタエントリにポリシールーティンググループ情報の設定がない場合，ポリシールーティングは行われま

せん。

フィルタエントリの Inbound 側フロー検出条件に一致した場合，ポリシールーティンググループ情報内のポリシールーティングリスト情報を優先度の高い順番に検索し，転送できるポリシールーティングリスト情報に設定された経路情報を使用してパケットを送信します。指定されたポリシールーティンググループ情報にパケットを転送できる経路がない（設定されたすべてのインタフェースが障害などによって使用できない）場合は，パケットは廃棄されます。

(1) パケットの転送例

次の図のようなネットワーク構成で，本装置のインタフェース Ia にポリシールーティングが設定されている場合の動作を示します。

図 11-33 ポリシールーティングパケット転送例 1

●インタフェースIaに設定したポリシールーティング
優先度1 ポリシー経路1（パケット送信できない）
優先度2 ポリシー経路2（パケット送信できる）
優先度3 ポリシー経路3（パケット送信できる）

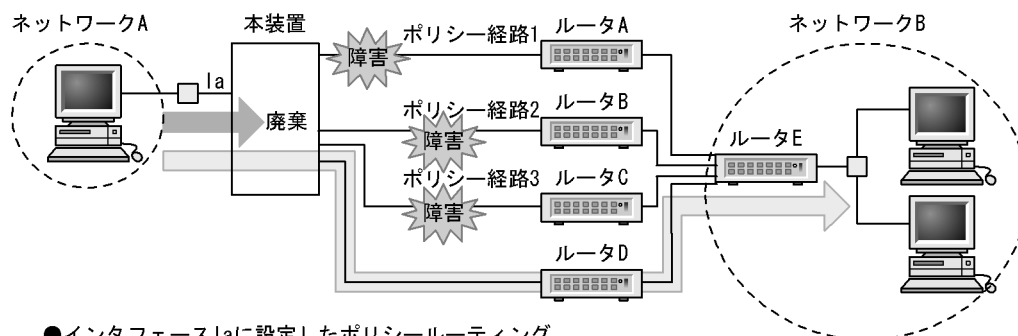
（凡例）：ポリシールーティングによるパケット転送経路
：ルーティングプロトコルによって決定したパケット転送経路

インタフェース Ia で受信したパケットが受信側のフィルタエントリの Inbound 側フロー検出条件に一致した場合，設定されているポリシールーティンググループ情報のポリシールーティングリスト情報を優先度の高い順番に検索し，パケットを送信できるポリシー経路（ポリシールーティングリスト情報に設定した経路）がある場合，その経路からパケットを送信します。「図 11-33 ポリシールーティングパケット転送例 1」ではポリシー経路 1，2，3 の順番に検索します。ポリシー経路 1 は障害によってパケットを送信できない状態なので，次に優先度の高いポリシー経路 2 を検索します。ポリシー経路 2 はパケットを送信できる状態なので，パケットはポリシー経路 2 に送信されます。

(2) パケットを破棄する例

次の図のようなネットワーク構成で，本装置のインタフェース Ia にポリシールーティングが設定されている場合の本装置の動作を示します。

図 11-34　ポリシールーティングパケット転送例 2

ネットワークA
本装置
Ia
廃棄
障害
ポリシー経路1
ルータA
ポリシー経路2
ルータB
障害
ポリシー経路3
ルータC
障害
ルータD
ルータE
ネットワークB

●インタフェースIaに設定したポリシールーティング
優先度1　ポリシー経路1（パケット送信できない）
優先度2　ポリシー経路2（パケット送信できない）
優先度3　ポリシー経路3（パケット送信できない）

（凡例）　：ポリシールーティングによるパケット転送経路
　　　　　：ルーティングプロトコルによって決定したパケット転送経路

インタフェース Ia で受信したパケットが受信側のフィルタエントリの Inbound 側フロー検出条件に一致した場合，設定されているポリシールーティンググループ情報のポリシールーティングリスト情報を優先度の高い順番に調べ，その結果ポリシールーティングリスト情報で設定しているすべてのインタフェースが障害などでパケットを転送できない場合は，該当するパケットを廃棄します。「図 11-34　ポリシールーティングパケット転送例 2」ではポリシー経路 1，2，3 の順番に検索し，すべてのポリシー経路が障害によってパケットを送信できないため，パケットを廃棄します。

このように，すべてのポリシールーティング経路が障害などの理由で中継できない状態の時は，パケットを廃棄します。本装置のポリシールーティング機能は，ルーティングプロトコルによる経路情報とは連動しません。

11.9.3　ポリシールーティング項目

ポリシールーティングの設定項目について示します。

（1） ポリシールーティングリスト情報

ポリシールーティングリスト情報の最大設定数は装置当たり 256 個です。ポリシールーティングリスト情報を次の表に示します。

表 11-22　ポリシールーティングリスト情報

設定項目	説明
ポリシールーティングリスト番号	ポリシールーティングリスト情報のエントリ番号。1 ～ 256 の範囲で指定します。
出力インタフェース名称	ip 情報で定義したパケットの出力先インタフェース名称。ただし，rmEthernet，AUX，トンネルは除きます。
ネクストホップ IP アドレス	パケットを送信するネクストホップ IP アドレス。
デフォルト指定	ポリシールーティンググループ情報に設定されている経路がすべてダウンしている場合に，使用する経路を指定します。

（2）ポリシールーティンググループ情報

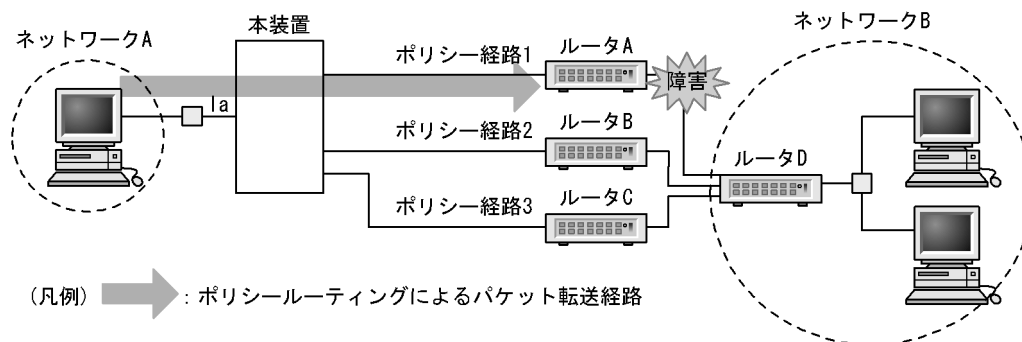
ポリシールーティンググループ情報の最大設定数は装置当たり 256 個です。また，全グループに登録されているポリシールーティングリスト情報の合計は最大 256 個です。ポリシールーティンググループ情報を次の表に示します。

表 11-23　ポリシールーティンググループ情報

設定項目	説明
ポリシールーティングリスト番号	ポリシールーティングリスト情報で定義したポリシールーティングリスト番号。
ポリシールーティンググループ名称	ポリシールーティングリスト情報を経路の優先順にグループ化するときのグループ名称。14 文字以内で指定します。

11.9.4　ポリシールーティング使用時の注意事項

1. ポリシールーティング機能は，リモートの経路が障害発生などでパケットを転送できない状態であっても検知する方法がないため，ポリシールーティングの経路を自動的に切り替えられません。例えば，次の図のように本装置にポリシールーティングが定義され，ネットワーク B 宛てのパケットに対してポリシー経路 1 が選択されている場合，ルータ A- ルータ D 間の経路が通信できない場合でも本装置はポリシー経路 1 に出力します。

図 11-35　ポリシールーティングパケット転送例 3

したがって，ポリシールーティング機能を使用する場合は，リモートの経路に障害が発生した場合でもパケットを迂回できるようなシステム構成にしてください。

2. ポリシールーティングを使用する場合，フロー検出条件パラメータに設定する IP_Source および IP_Destination には次に示す IPv4 アドレスを設定してください。
   ClassA: 1.0.0.1 ～ 126.255.255.254
   ClassB: 128.1.0.1 ～ 191.254.255.254
   ClassC: 192.0.1.1 ～ 223.255.254.254
   127.0.0.0 ～ 127.255.255.255 の IPv4 アドレス，クラス D の IPv4 アドレス (224.0.0.0 ～ 239.255.255.255)，ブロードキャストアドレス (net ID および host ID が 2 進数ですべて 1 またはすべて 0) は設定しないでください。
3. ポリシールーティングの出力先インタフェース名称がリンクアグリゲーションの場合，Inbound 側の flow filter 条件を設定するインタフェースが搭載される PSU または BSU は以下をご使用ください。
   ［PSU］：PSU-12，PSU-22，PSU-33，PSU-43
   ［BSU］：BSU-S2，BSU-C2
4. ポリシールーティング機能で代替経路への切り替えは，現在使用しているポリシールーティングリスト情報のインタフェースがダウンした場合に行われます。インタフェースのダウン契機について以下に示

します。

［インタフェースのダウン契機］

- インタフェースが定義されている物理回線 (VLAN およびリンクアグリゲーション使用時は所属する全物理回線) がリンクダウンした場合
- インタフェースが定義されている物理回線が close コマンドによって閉塞された場合
- インタフェースが定義されている物理回線がコンフィグレーションコマンド disable によって閉塞された場合
- インタフェースが定義されている物理回線で，リスタートが必要なコンフィグレーションが追加／変更された場合

5. PSU-1，PSU-2，BSU-C1 および BSU-S1 以降使用時，ポリシールーティング機能が動作可能なパケット種別を以下に示します。

   ［IPv4 パケット］

   - 自宛 MAC アドレス＋自宛 IP ユニキャストアドレス
   - 自宛 MAC アドレス＋他宛 IP ユニキャストアドレス
   - 自宛 MAC アドレス＋ IP サブネットブロードキャストアドレス

   ［IPv6 パケット］

   - 自宛 MAC アドレス＋自宛 IPv6 ユニキャストアドレス
   - 自宛 MAC アドレス＋他宛 IPv6 ユニキャストアドレス

6. 以下の NIF についてポリシールーティング機能は未サポートです。
   - NP192-1S4
   - NP192-1S
   - NP48-4S

7. プライベート VLAN 機能を使用している VLAN に対するポリシールーティング機能は未サポートです。
8. 本装置でサポートする各種プロトコルの制御パケットは，ポリシールーティングの対象外です。フィルタリング機能および QoS 制御機能を運用するに当たって，フロー検出条件オプション 1 機能を指定した場合でも同じです。

11.10 DHCP/BOOTP リレーエージェント機能

DHCP/BOOTP リレーエージェント機能とは，DHCP/BOOTP サーバ (以降，サーバという) と DHCP/BOOTP クライアント (以降，クライアントという) が異なるサブネットにある場合，コンフィグレーションで設定した Relay Address(サーバの IP アドレス，またはサーバが存在しているネットワークへ中継できるルータの IP アドレス) を DHCP/BOOTP パケットの宛先 IP アドレスに設定し，サーバへ該当するパケットをサブネット間中継する機能です。この節では本装置の DHCP/BOOTP リレーエージェント機能の仕様および動作内容について示します。

11.10.1 サポート仕様

DHCP/BOOTP クライアント接続セグメントは 1 論理インタフェースに一つ設定できます。DHCP/BOOTP クライアントが接続されているインタフェースにマルチホームを設定している場合，コンフィグレーションコマンド relay-interface の relay_agent_address パラメータを省略すると DHCP/BOOTP クライアントが接続されている IP アドレス (リレーエージェントアドレス) は IP 定義の最後に設定する必要があります。

設定方法の詳細については，「コンフィグレーションガイド　8.4.4 DHCP/BOOTP クライアントへの接続をマルチホームインタフェースとする」を参照してください。

また，DHCP/BOOTP リレーと VRRP 機能を同一インタフェースで運用する場合は，DHCP/BOOTP サーバで，DHCP/BOOTP クライアントゲートウェイアドレス (ルータオプション) を仮想ルータアドレスに設定する必要があります。設定方法の詳細については，「コンフィグレーションガイド　8.4.6 DHCP/BOOTP リレーと VRRP 連携」を参照してください。

11.10.2 DHCP/BOOTP パケットを受信したときのチェック内容

DHCP/BOOTP パケットを受信したときのチェック内容を次の表に示します。IP ヘッダのチェック内容は「11.4　通信機能」を参照してください。

表 11-24　DHCP/BOOTP パケットを受信したときのチェック内容

DHCP/BOOTP パケットヘッダフィールド	チェック内容	チェック NG 時パケット廃棄	
		クライアント→サーバ	サーバ→クライアント
BOOTP REQUEST HOPS	コンフィグレーションの設定値より小さいこと	廃棄する	廃棄しない
リレーエージエントアドレス	本装置宛てであること	廃棄する	廃棄する
IP ヘッダ TTL	1 より大きいこと	廃棄する	廃棄する
IP ヘッダ送信元アドレス	ネットワーク番号が 0 でないこと	廃棄しない	廃棄する

11.10.3 中継時の設定内容

DHCP/BOOTP リレーエージェント機能が DHCP/BOOTP パケットを中継するときの設定内容を次の表に示します。

表 11-25　DHCP/BOOTP 中継時の設定内容

パケットヘッダフィールド	設定条件	条件を満たす場合に設定する内容	
		クライアント→サーバ	サーバ→クライアント
DHCP/BOOTP ヘッダリレーエージェントアドレス	0.0.0.0 の時	• 受信インタフェースにマルチホームの設定がない場合，受信インタフェースの IP アドレスを設定します。 • 受信インタフェースにマルチホームの設定がある場合，運用コマンドの show dhcp giaddr コマンドで表示される IP アドレスを設定します。※1	-
DHCP/BOOTP ヘッダブロードキャストフラグ	1 のとき	-	宛先 IP アドレスを制限付きブロードキャスト※2に設定します。
	0 のとき	-	宛先 IP アドレスをクライアント IP アドレスに設定します。 宛先 MAC アドレスをクライアントハードウェアアドレスに設定します。
DHCP/BOOTP ヘッダBOOTP REQUEST HOPS	DHCP/BOOTP REQUEST パケットを DHCP/BOOTP サーバへ中継するとき	1 増加させます。	-
IP ヘッダ送信元アドレス	0.0.0.0 のとき	送信インタフェースの IP アドレスを設定します。	-
IP ヘッダ宛先アドレス	制限付きブロードキャスト※2のとき	Relay Address を設定します。	-

（凡例）　- : 該当しない

注※ 1

show dhcp giaddr interface< 受信インタフェース名 > と入力すると，DHCP/BOOTP パケットフィールドのリレーエージェントアドレスに設定する IP アドレスが表示されます。

show dhcp giaddr コマンドについては，マニュアル「運用コマンドレファレンス Vol.2」を参照してください。

詳細については「11.10.4　ネットワーク構成例　(4) DHCP/BOOTP クライアント接続インタフェースにマルチホーム設定がある構成例」を参照してください。

注※ 2

IP ブロードキャストアドレスで，255.255.255.255 または 0.0.0.0 の形式を持つ IP アドレスを示します。

11.10.4　ネットワーク構成例

DHCP/BOOTP リレーエージェント機能を使用したネットワーク構成例を示します。

(1) DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが 1 台ある構成例

DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが 1 台ある場合の構成例を次の図に示します。

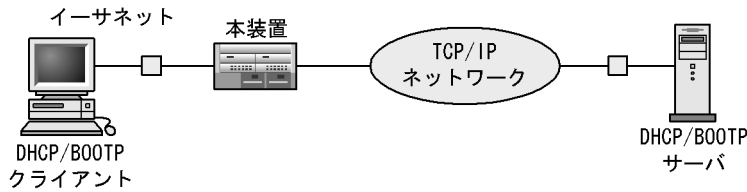
図 11-36 構成例 1(DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが 1 台ある場合)

この図のリレーエージェント設定項目を次の表に示します。

表 11-26 リレーエージェント設定項目 (構成例 1)

設定項目		設定値
DHCP/BOOTP クライアント接続側のインタフェース	BOOTP REQUEST HOPS	1(経由するリレーエージェント最大数)
	Relay Address	DHCP/BOOTP サーバの IP アドレス
DHCP/BOOTP サーバ側インタフェース	なし	-

(凡例) - : 該当しない

(2) DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある構成例 (DHCP/BOOTP サーバの IP アドレスが既知の場合)

DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある場合の構成例を次の図に示します。DHCP/BOOTP クライアント側ネットワークで，DHCP/BOOTP サーバの IP アドレスが既知の場合に有効です。

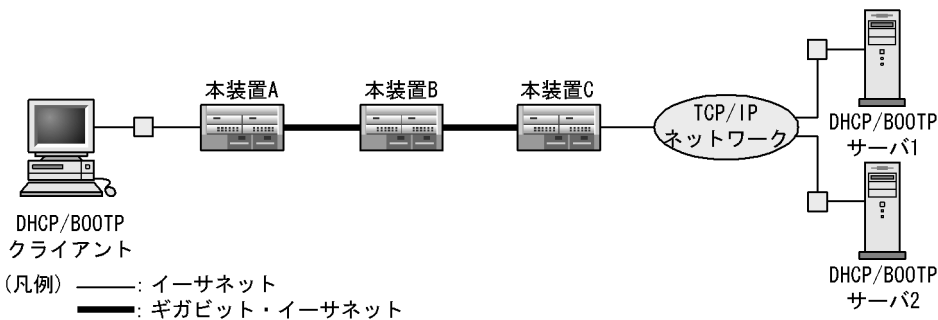
図 11-37 構成例 2(DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある場合)

この図の本装置 A，B，C の各リレーエージェント設定項目を次の表に示します。

表 11-27 リレーエージェント設定項目 (構成例 2)

装置	設定項目		設定値
本装置 A	DHCP/BOOTP クライアント接続側のインタフェース	BOOTP REQUEST HOPS	1(経由するリレーエージェントの最大数)

装置	設定項目		設定値
		Relay Address	• DHCP/BOOTP サーバ 1 の IP アドレス • DHCP/BOOTP サーバ 2 の IP アドレス
	本装置 B とのインタフェース	なし	-
本装置 B	本装置 A とのインタフェース	なし	-
	本装置 C とのインタフェース	なし	-
本装置 C	本装置 B とのインタフェース	なし	-
	DHCP/BOOTP サーバ 接続側のインタフェース	なし	-

(凡例)　- : 該当しない

(3) DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある構成例 (DHCP/BOOTP サーバの IP アドレスが不明の場合)

DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある場合の構成例を次の図に示します。DHCP/BOOTP クライアント側ネットワークで，DHCP/BOOTP サーバの IP アドレスが不明な場合に有効です。

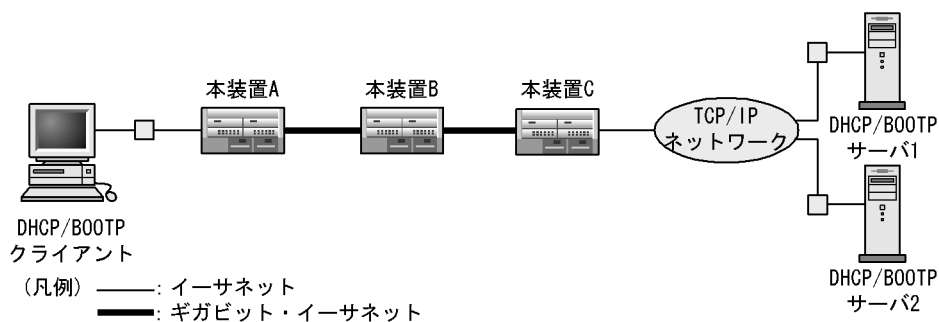
図 11-38　構成例 3(DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが複数台ある場合)

この図に示す本装置 A，B，C の各リレーエージェント設定項目を次の表に示します。

表 11-28　リレーエージェント設定項目 (構成例 3)

装置	設定項目		設定値
本装置 A	DHCP/BOOTP クライアント 接続側のインタフェース	BOOTP REQUEST HOPS	1(経由するリレーエージェントの最大数)
		Relay Address	本装置 B の本装置 A とのインタフェース IP アドレス
	本装置 B とのインタフェース	なし	-
本装置 B	本装置 A とのインタフェース	BOOTP HOPS	2
		Relay Address	本装置 C の本装置 B とのインタフェース IP アドレス
	本装置 C とのインタフェース	なし	-
本装置 C	本装置 B とのインタフェース	BOOTP HOPS	3

装置	設定項目		設定値
		Relay Address	• DHCP/BOOTP サーバ 1 の IP アドレス • DHCP/BOOTP サーバ 2 の IP アドレス
	DHCP/BOOTP サーバ接続側のインタフェース	なし	-

（凡例） - : 該当しない

（4） DHCP/BOOTP クライアント接続インタフェースにマルチホーム設定がある構成例

DHCP/BOOTP リレーエージェント機能では，クライアントからの IP アドレス貸し出し要求パケット (DHCP/BOOTP REQUEST パケット) を受信したとき，受信インタフェースの IP アドレスをリレーエージェントアドレスとしてパケットに設定し，サーバへ中継します。ただし，本装置でクライアント接続インタフェースにマルチホームの設定がある場合，コンフィグレーションコマンド relay-interface の relay_agent_address パラメータを省略するとインタフェースに最後に IP 定義した IP アドレスをパケットに設定しています。DHCP/BOOTP クライアント接続インタフェースにマルチホーム設定がある場合の構成例を次の図に示します。

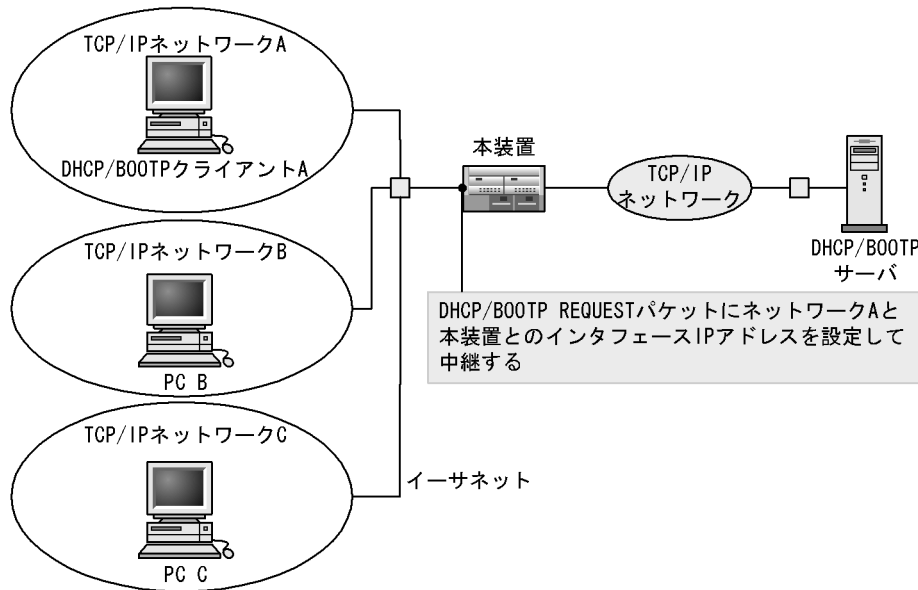
図 11-39 構成例 4

この図のリレーエージェント設定項目を次の表に示します。

表 11-29 リレーエージェント設定項目 (構成例 4)

設定項目		設定値
DHCP/BOOTP クライアント側インタフェース	IP アドレス	ネットワーク B，ネットワーク C と本装置とのインタフェース IP アドレス
		ネットワーク A と本装置とのインタフェース IP アドレス※
	BOOTP REQUEST HOPS	1(経由するリレーエージェント最大数)

設定項目		設定値
	Relay Address	DHCP/BOOTP サーバの IP アドレス
DHCP/BOOTP サーバ側インタフェース	なし	-

（凡例） - : 該当しない

注※　コンフィグレーションコマンド relay-interface の relay_agent_address パラメータを省略すると最後に設定する必要があります。設定方法の詳細については「コンフィグレーションガイド　8.4.4 DHCP/BOOTP クライアントへの接続をマルチホームインタフェースとする」を参照してください。

(5) リレーエージェント情報オプション (Option82) を有効にする構成例

DHCP リレーエージェント情報オプション (Option82) は，DHCP/BOOTP リレーエージェントで要求パケットを中継する際に，リレーエージェント固有の情報を追加してから転送するためのオプションです。追加する情報はリレーエージェント情報オプション (オプションコード : 82) として DHCP オプションの最後に追加されます。また，次に示す形式でサーキット ID とリモート ID の二つのサブオプションを含みます。

なお，応答パケットを転送する場合は，リレーエージェント情報オプションを削除してからクライアントに転送します。

(a) サーキット ID

装置ごとの要求元の回線を識別するための ID です。クライアントが接続されている回線の情報（VLAN ID，および NIF 番号 /LINE 番号またはリンクアグリゲーショングループ ID）が設定されます。

注※　LA-Mode：NIF番号/LINE番号指定=0，リンクアグリゲーショングループID=1

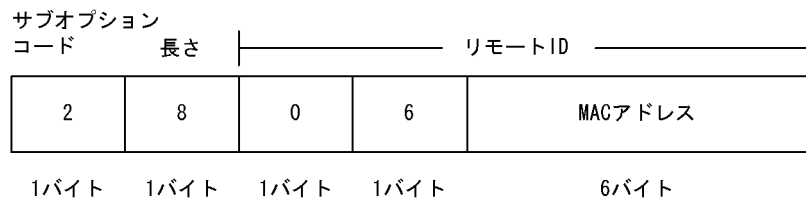
(b) リモート ID(port_unique 指定時)

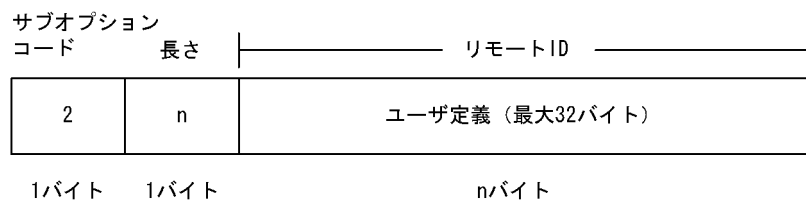
要求元を識別するための ID です。装置を識別するための MAC アドレス（装置 MAC アドレス）とクライアントが接続されている回線の情報を組み合わせているため，ネットワーク上で一意の値になります。

注※　LA-Mode：NIF番号/LINE番号指定=0，リンクアグリゲーショングループID=1

(c) リモート ID(mac_address 指定時)

装置を識別するための ID です。本装置の装置 MAC アドレスが設定されます。クライアントごとの制御

を行う場合は DHCP サーバ側でサーキット ID と組み合わせる必要があります。

(d) リモート ID(user_define 指定時)

装置を識別するための ID です。装置 MAC アドレスの代わりに，コンフィグレーションで設定した任意のバイナリデータを使用します。

注意事項

リモート ID はコンフィグレーションによって，(b) ～ (d) の 3 種類の中から選択します

DHCP サーバはこのサブオプションの内容によって動作を決定します。具体的には，リモート ID ごとに IP アドレスを固定で割り振ることで MAC アドレスに依存しない固定 IP アドレス割り当てなどを可能にします。

本機能は転送時に情報を追加するだけで，追加されたデータの利用方法は DHCP サーバに依存します。また，DHCP サーバ側がリレーエージェント情報オプションに対応していない場合，DHCP サーバは本オプションを無視します。

DHCP/BOOTP リレーエージェント情報オプション (Option82) を有効に設定する構成例を次の図に示します。

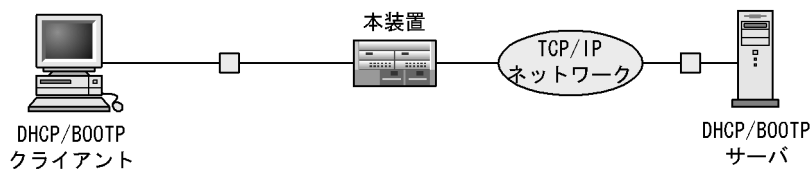
図 11-40　構成例 5

この図のリレーエージェント設定項目を次の表に示します。

表 11-30 リレーエージェント設定項目 (構成例 5)

設定項目		設定値
DHCP/BOOTP クライアント側インタフェース	BOOTP REQUEST HOPS	1(経由するリレーエージェント最大数)
	Relay Address	DHCP/BOOTP サーバの IP アドレス
	リレーエージェント情報ポリシー	生成するリモート ID の形式
DHCP/BOOTP サーバ側インタフェース	なし	-

(凡例) - : 該当しない

11.10.5 DHCP/BOOTP リレーエージェント機能使用時の注意事項

1. DHCP/BOOTP リレーエージェント機能と VRRP 機能を同一インタフェースで同時に運用する場合は，DHCP/BOOTP サーバで，DHCP/BOOTP クライアントゲートウェイアドレス (ルータオプション) を本装置に設定した仮想ルータアドレスに設定する必要があります。設定方法の詳細については，「コンフィグレーションガイド 8.4.6 DHCP/BOOTP リレーと VRRP 連携」を参照してください。
2. DHCP リレーエージェント情報オプション (Option82) 機能を二重化で運用する場合は，コンフィグレーションで装置 MAC アドレスを設定してください（user_define 指定時は除きます)。**【SB-7800S】**

11.11　DHCP サーバ機能

DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。この節では本装置の DHCP サーバ機能の仕様および動作内容を説明します。

11.11.1　サポート仕様

本装置の DHCP サーバ機能のサポート仕様を次の表に示します。DHCP サーバとクライアント接続は，同一ネットワーク内での直結，および DHCP リレーエージェント経由で行います。なお，DHCP サーバがクライアントに割り当てできる IP アドレスは最大で SB-7800S の場合 8,192，SB-5400S の場合 2,000 個です。

表 11-31　DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	• DHCP クライアントを直接収容 • DHCP リレーエージェント経由で収容
サポートメディア※1※2	イーサネット（1Gbit/10Gbit を含む）
最大リース IP アドレス	• SB-7800S の場合 DHCP クライアント 8,192 台 • SB-5400S の場合 DHCP クライアント 2,000 台
ネットワーク層プロトコル	IPv4 だけに対応しています。※3
BOOTP 対応	対応していません。
DynamicDNS 連携※4	対応しています。

注※ 1

Tag-VLAN 連携，またはマルチホーム（複数 IP アドレス／インタフェース）接続もサポートします。マルチホーム接続では，マルチホームしている物理回線に最初にコンフィグレーションに定義された IP アドレスを入力インタフェースの IP アドレスとします。このサブネットに定義しているアドレスプールから IP アドレスを DHCP クライアントに割り当てます。

注※ 2

POS 回線は，リレーエージェント経由で収容する場合でも使用できません。

注※ 3

IPv6 DHCP サーバとの同時動作は可能です。

注※ 4

本装置で対応しているのは DNS UPDATE を使用した DynamicDNS サーバです。

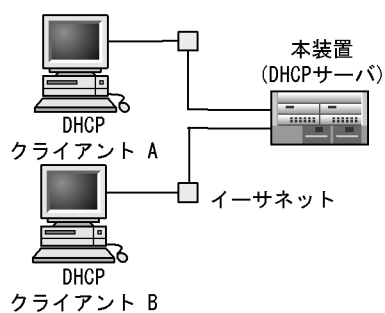
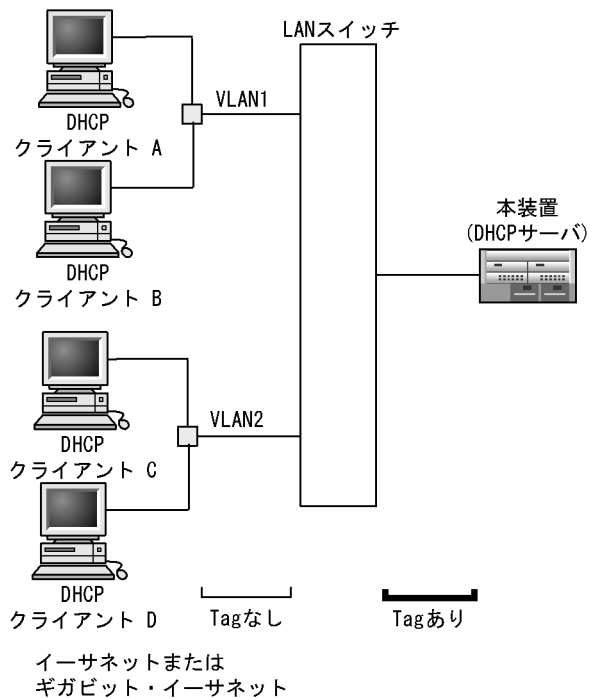
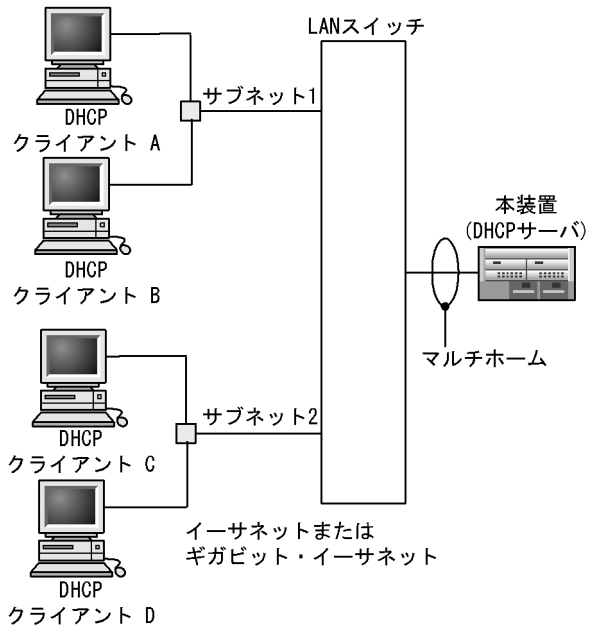
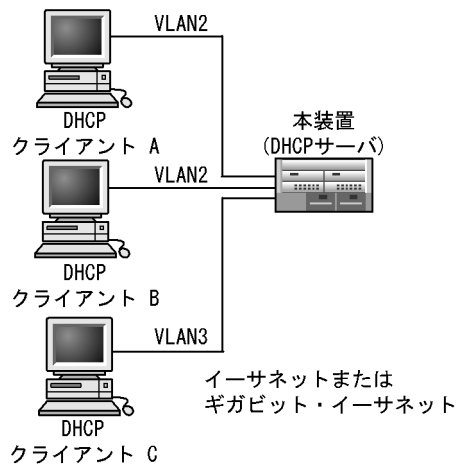
11.11.2　接続構成

本装置でサポートする DHCP サーバ機能の接続構成について説明します。

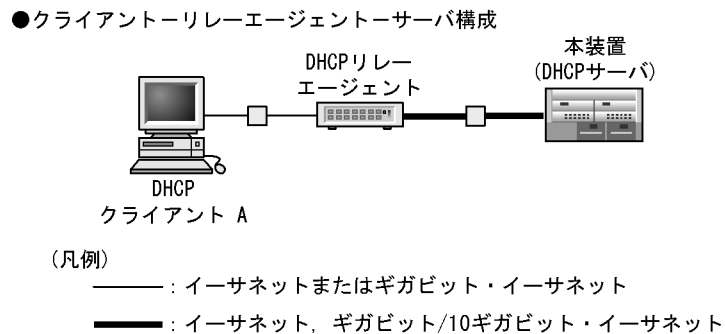
（1）クライアントを直接収容する場合

クライアントを直接収容する場合の接続構成を次の図に示します。

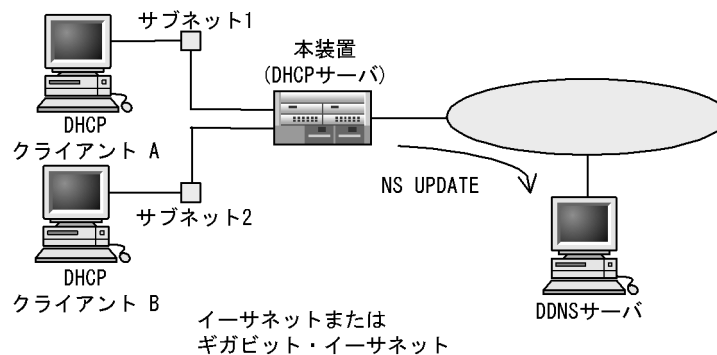
図 11-41　クライアントを直接収容する場合の接続構成

●クライアント−サーバ構成：本装置側インタフェース

●Tag-VLAN連携でのクライアント−サーバ構成

●マルチホームでのクライアント－サーバ構成

●スイッチポートでのクライアント－サーバ構成

(2)　リレーエージェントを経由する場合

リレーエージェントを経由する場合の接続構成を次の図に示します。

図 11-42　リレーエージェントを経由する場合の接続構成

（3） DynamicDNS 連携を行う場合

DynamicDNS 連携を行う場合の接続構成を次の図に示します。

図 11-43　DynamicDNS 連携を行う場合の接続構成

11.11.3　クライアントへの配布情報

本装置でクライアントへ配布可能な情報の一覧を次の表に示します。配布可能な情報の中でオプション扱いの情報については，本装置で配布するオプションを指定した場合でも，クライアント側からオプション要求リストによって要求しない場合は配布データに含めません。

表 11-32　本装置でクライアントに配布する情報の一覧

情報名	概要
IP アドレス	クライアントが使用可能な IP アドレスを設定します。
IP アドレスリース時間	配布する IP アドレスのリース時間を設定します。本装置では default-lease-time/ max-lease-time パラメータとクライアントからの要求によって値が決定されます。(Option No : 51)
サブネットマスク	本オプションは配布する IP アドレスのサブネットマスクを指定するときに使用します。この情報を指定しない場合はサブネット情報定義のサブネットマスク長が使用されます。(Option No : 1)
ルータオプション	クライアントのサブネット上にあるルータの IP アドレスのリストを指定します。リストは優先度の高いものから順に指定します。このリストがクライアントのゲートウェイアドレスとして使用されます。(Option No : 3)
DNS オプション	クライアントが利用できるドメインネームサーバの IP アドレスのリストを指定します。リストは優先度の高いものから順に指定します。(Option No : 6)

情報名	概要
ホストネームオプション	サーバでクライアントの名前を指定するときに設定します。名前はローカルドメイン名で制限される可能性があります。指定は文字列で行われます。(Option No : 12)
ドメイン名オプション	クライアントがドメインネームシステムによってホスト名を変換するときに使用するドメイン名を指定します。(Option No : 15)
NetBIOS over TCP/IP ネームサーバオプション	クライアントが参照する NetBIOS ネームサーバ (WINS サーバ) を IP アドレスのリストで指定します。リストは優先度の高いものから順に指定します。(Option No : 44)
NetBIOS over TCP/IP ノードタイプ指定オプション	NetBIOS オーバ TCP/IP クライアントのノードタイプ (NetBIOS 名前解決方法) を設定します。(Option No : 46) • コード１　B ノード (ブロードキャストノード) • コード２　P ノード (Peer to Peer ノード (WINS を使用)) • コード４　M ノード (ミックスノード (ブロードキャストで見つからない場合に WINS を使用する)) • コード８　H ノード (ハイブリッドノード (WINS で見つからない場合に，ブロードキャストを使用する))
SMTP サーバオプション	クライアントが利用できる SMTP サーバを優先されるものから順に IP アドレスリストで指定します。(Option No : 69)
POP3 サーバオプション	クライアントが利用できる POP3 サーバを優先されるものから順に IP アドレスリストで指定します。(Option No : 70)

11.11.4　DHCP サーバ機能使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

(1)　割り当て用 IP アドレスの使用状況の確認

本装置で接続できるクライアントの台数（IP アドレスプールの数）は SB-7800S の場合 8,192 台，SB-5400S の場合 2,000 台です。IP アドレスプールで空き状態となっている個数は，show ip dhcp server statistics コマンドの実行結果「address pools」で確認できます。また，実際に割り当てられた IP アドレスは，show ip dhcp binding コマンドで確認できます。各コマンドについては，マニュアル「運用コマンドレファレンス Vol.2」を参照してください。

(2)　二重化 RM 切り替え後やサービス中の本装置再立ち上げ後の動作

本装置のサービス (DHCP クライアントにアドレスを割り当てた状態) 中に RM 二重化切り替えや本装置がダウン (RM 二重化構成時は二重障害) 後に装置再立ち上げで復帰した場合，本装置上にある割り当て用 IP アドレスのプールはすべて「空き状態」になります。しかし，その後本装置が IP アドレスを割り当てる際，事前に割り当てた IP アドレスに対して ICMP エコー要求パケットを送出し，その応答パケットの有無によってすでに使用しているクライアントがいないかを確認し，IP アドレスの二重割り当てを防止します。同時に，以前 IP アドレスを割り当てたクライアントに対しては同じ IP アドレスを割り当てようとするため，二重化 RM 切り替えや本装置を再立ち上げした場合もクライアントの通信には影響を与えません。

また，ICMP エコー要求パケットの応答が返ってきた (ネットワーク上の端末がすでにその IP アドレスを使っている) 場合，show ip dhcp conflict コマンド (マニュアル「運用コマンドレファレンス Vol.2」を参照してください) の実行結果画面に矛盾アドレス検出として表示します。

11.11.5　DynamicDNS 連携に関して

本装置の DHCP サーバは IP アドレス配布と同時に DynamicDNS サーバに対してエントリレコードを追

加する機能（DNS 更新）に対応しています。本装置は DNS UPDATE によってエントリレコードを更新できる DynamicDNS サーバに対応しています。この機能を使用するには本装置で対象とするゾーンと要求先 DNS サーバを指定した上で，DNS サーバ側も本装置からのレコード更新を受け付けるように設定する必要があります。

レコード更新の許可には IP アドレスによる許可と HMAC-MD5 の認証キーを使用する方法があります。IP アドレスによる許可は DNS サーバに接続している IP アドレスまたはネットワークからのアクセスを DNS サーバ側で許可するだけですが，認証キーを使用する場合は DNS サーバで指定されたキーと同じキーを本装置の DNS 認証キー情報に設定する必要があります。

DynamicDNS 連携時の注意事項

- 本装置では動的に割り当てる IP アドレスだけ DNS 更新を行います。固定アドレスで配布を行う場合は事前に DNS にレコードを追加してください。
- DNS 更新を行うには IP アドレス配布時にクライアントが FQDN をサーバに返す必要があります。必要な情報がない場合，DHCP サーバはそのリースに対する DNS 更新を行いません。具体的には，WindowsXP では TCP/IP 詳細設定の DNS に関する項目で「この接続のアドレスを DNS に登録する」にチェックをつける必要があります。
- DNS 更新で認証キーを使用する場合，DNS サーバと本装置の時刻情報が一致している必要があります。多くの場合，時刻情報の誤差は UTC 時間で 5 分以下である必要があるため，NTP による時刻情報の同期を行ってください。

11.12 DNS リレー機能

DNS リレー機能 (DNS プロキシ機能) は，DNS(Domain Name System) クライアントと DNS サーバが異なるサブネットに存在する時，DNS クライアントからの DNS パケットを本装置のコンフィグレーションで設定したネームサーバのアドレスにサブネット間中継する機能です。

11.12.1 サポート仕様

本装置の DNS リレー機能のサポート仕様を次の表に示します。なお DNS リレー収容できるクライアント台数は最大 2000 個です。

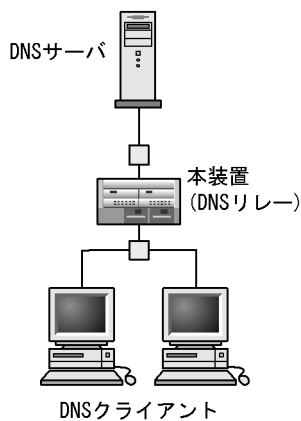
表 11-33 DNS リレー機能のサポート仕様

項目	仕様
接続構成	• DNS クライアントを直接収容する • DNS リレー機能がある装置を収容する
ネットワーク層プロトコル※	• IPv4 だけサポートする

注※ IPv4 パケットを利用した IPv6 フォーマット (クワッド・エー) のアドレスおよびドメインは，本装置を使用して中継できます。

11.12.2 接続構成

DNS リレー機能の接続構成を次の図に示します。

図 11-44 DNS リレー機能の接続構成 (クライアントを直接収容する場合)

（凡例）―――：10M／100Mイーサネットまたはギガビット・イーサネット

11.12.3 コンフィグレーションによる動作内容

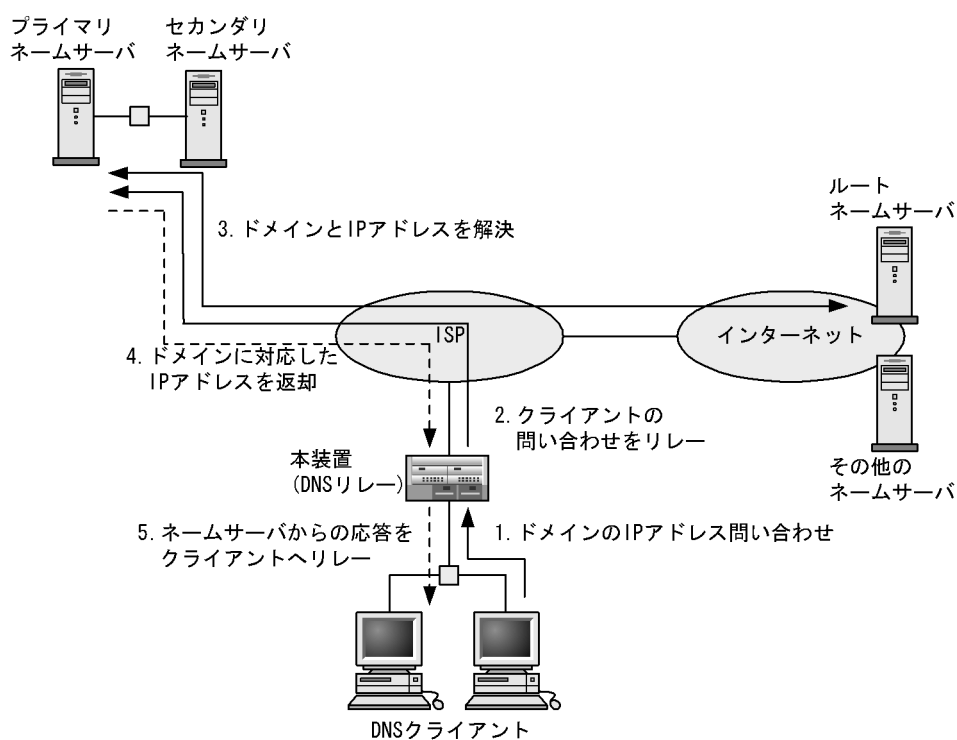
ネームサーバの IP アドレスは，コンフィグレーションで設定します。コンフィグレーションの内容ごとの動作を次の表に示します。

表 11-34　コンフィグレーションの内容ごとの動作

コンフィグレーション	動作内容
コンフィグレーションでネームサーバの IP アドレスとリレー有効を設定	DNS リレー機能は動作する コンフィグレーションに設定してあるネームサーバのアドレスを使用する
コンフィグレーションでリレー有効だけを設定	• DNS リレー機能は動作する

11.12.4　ネットワーク構成例

本装置でサポートする DNS リレー機能を使用したネットワーク構成例を次の図に示します。

図 11-45　DNS リレー機能を使用したネットワーク構成例

（1）

12 RIP ／ OSPF

本章では，IPv4 のルーティングプロトコルの RIP，OSPF について説明します。

12.1　IPv4 ルーティング

IPv4 ルーティングプロトコルの概要について説明します。

12.1.1　スタティックルーティングとダイナミックルーティング

パケットを中継するためにはルーティングテーブルを作成する必要があります。本装置のルーティングテーブルの作成方法は，大きく**スタティックルーティング**と**ダイナミックルーティング**に分類できます。

- スタティックルーティング
  ユーザがコンフィグレーションによって経路情報を設定する方法です。
- ダイナミックルーティング
  ネットワーク内のほかのルータと経路情報を交換して中継経路を決定する方法です。本装置は RIP バージョン 1 およびバージョン 2，OSPF バージョン 2，BGP バージョン 4，IS-IS をサポートしています。

12.1.2　経路情報

本装置が取り扱う経路情報（ルーティングの対象とするアドレスの種類）を次の表に示します。

表 12-1　経路情報

経路情報		説明
通常の経路	デフォルト経路	すべてのネットワーク宛ての経路。 （宛先アドレス：0.0.0.0，ネットワークマスク：0.0.0.0）
	ナチュラルマスク経路	アドレスクラスに対応したネットワークマスクの経路。 （ネットワークマスク：クラス A ＝ 8 ビット，クラス B ＝ 16 ビット，クラス C ＝ 24 ビット）
	サブネット経路	特定のサブネット宛ての経路。 （ネットワークマスクがアドレスクラスに対応したネットワークマスクよりも長い経路）
	ホスト経路	特定のホスト宛ての経路。 （ネットワークマスクが 32 ビットの経路）
	可変長サブネットマスク	可変長サブネットマスク：VLSM(Variable Length Subnet Mask) を取り扱います。同一ネットワークアドレスで，長さの異なる複数のサブネットマスクを取り扱えます。
CIDR 対応の経路	スーパーネット経路	アドレスクラスに対応したネットワークマスクより短いネットワークマスクの経路情報を取り扱えます。例えば，クラス C のネットワークアドレス 192.168.8.0/24，192.168.9.0/24，192.168.10.0/24，192.168.11.0/24 の経路情報を一つのスーパーネット経路 192.168.8.0/22 に集約し取り扱えます。
	0 サブネット経路	サブネット番号が 0 のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば，クラス B のネットワークアドレス 172.16.0.0/24 の経路情報を取り扱えます。
	-1 サブネット経路	サブネット番号が -1(All'1') のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば，クラス B のネットワークアドレス 172.16.255.0/24 の経路情報を取り扱えます。
	包括的サブネット	複数の経路情報間でネットワークアドレスが包括関係にある経路を別の経路情報として取り扱います。例えば，クラス B のネットワークアドレス 172.16.3.0/24 と 172.16.2.0/23 は個々の経路情報として取り扱えます。

12.1.3　ルーティングプロトコルごとの適用範囲

本装置のサポートするルーティングプロトコルごとの適用範囲を次の表に示します。

表 12-2　ルーティングプロトコルごとの適用範囲

経路情報		ルーティング			
		スタティック	ダイナミック		
			RIP-1	RIP-2	OSPF
経路情報	デフォルト経路	○	○	○	○
	ナチュラルマスク経路	○	○	○	○
	サブネット経路	○	○	○	○
	ホスト経路	○	○	○	○
	可変長 サブネットマスク	○	×	○	○
	CIDR 対応	○	△	○	○
	マルチパス (最大 16 パス)	○	×	×	○
経路選択		-	メトリック (経由するルータ数)		コスト (経由するルータ数および回線速度)
ルーティングループ抑止		-	スプリットホライズン		○
認証機能		-	×	×	○

(凡例)

○：取り扱う

△：一部取り扱う (0 サブネット経路，-1 サブネット経路は取り扱う)

×：取り扱わない

-：該当しない

12.2 ネットワーク設計の考え方

この節では RIP/OSPF を使用して IPv4 ネットワークを設計する場合の考え方について説明します。

12.2.1 アドレス設計

ローカルアドレスを使用する場合で IP アドレスの割り当てに余裕がある場合には，次のような考え方に従うと注意事項の多くを回避でき，比較的簡単なネットワーク設計になります。

1. 複数のネットワークアドレスを使用しないで，大きな単一のネットワークアドレス (ClassA または ClassB) をサブネット化して使用し，アドレス境界を作らないようにします。
2. サブネットマスクのビット数は同一とします (可変長サブネットマスクにならないようにします)。
3. ポイント - ポイント型の回線にも一つのサブネット分の IP アドレスを割り当てます。

1 および 2 のアドレッシング条件に合わず，RIP-1 によるルーティングを行う場合，経路広告条件に注意が必要です。

12.2.2 直結経路の取り扱い

本装置はブロードキャスト型の回線 (イーサネット) とポイント - ポイント型の回線で経路情報 (直結経路) の扱いが異なります。

ブロードキャスト型の場合はネットワークアドレス (NA) とサブネットマスク (Mask) として扱います (「図 12-1　直結経路の取り扱い (ブロードキャスト型の場合)」参照)。

ポイント - ポイント型の場合は二つの IP アドレス a，b として扱います (「図 12-2　直結経路の取り扱い (ポイント - ポイント型の場合)」参照)。

図 12-1　直結経路の取り扱い (ブロードキャスト型の場合)

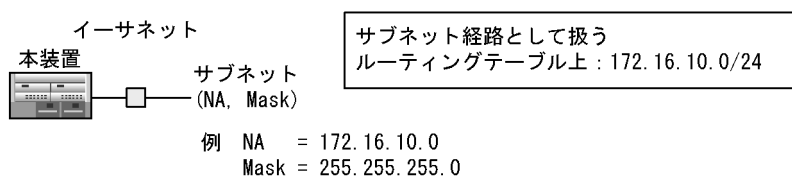
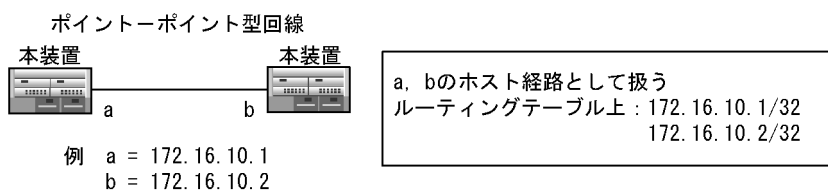



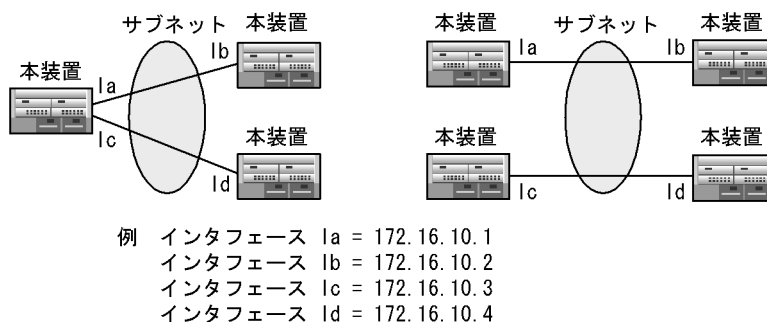
図 12-2　直結経路の取り扱い (ポイント - ポイント型の場合)

(a) ポイント - ポイント型回線のダイレクト経路の広告

ポイント - ポイント型回線のダイレクト経路はホスト経路として生成されます。したがって，ポイント - ポイント型回線のダイレクト経路は二つのホスト経路として広告されます。本装置では，コンフィグレーションコマンド options の gen-prefix-route パラメータを指定することによって，ポイント - ポイント型回線のダイレクト経路を一つのネットワーク経路として広告できます。なお，このパラメータを指定した場合は，該当するダイレクト経路のホスト経路は広告対象外です。

(b) 複数のポイント - ポイント型回線に同一サブネットの IP アドレスを割り当てる場合

ポイント - ポイント型回線の場合はホスト経路としてアドレス情報を管理します。したがって，本装置だけで構成されたネットワークでは次の図に示すように異なるポイント - ポイント型回線に同一サブネットのアドレスを割り当てることもできます。

図 12-3　ポイント - ポイント型回線での同一サブネットアドレス割り当て

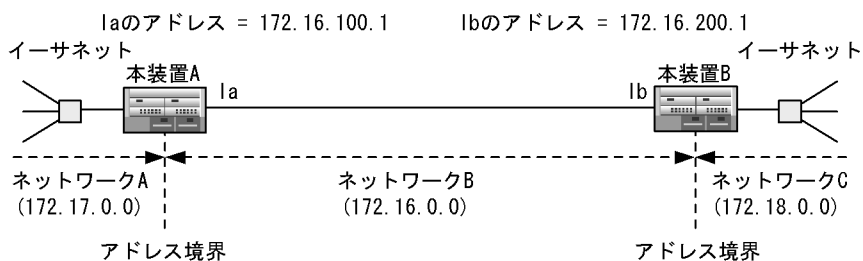
利点

IP アドレスを節約できます。

制限事項

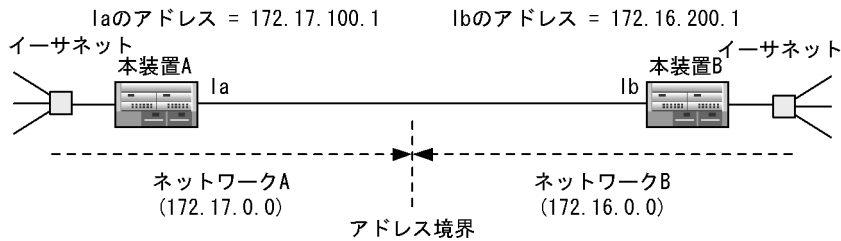
- 本装置間だけでできます。そのほかのルータ間では使用しないでください。
- SNMP を使用したネットワーク管理装置でのネットワーク構成の自動描画は物理回線と一致しなくなります (同一サブネット内の回線がまたがって一つ表示されます)。

12.2.3　アドレス境界の設計

複数のネットワークアドレスを使用する場合は，次の図に示すように本装置上にアドレス境界を置くようにしてください。アドレス境界とはナチュラルマスクに対応したネットワークアドレスの境界を意味します。アドレスクラスの境界ではありません。

図 12-4　通常のアドレス境界設計例

(1) ポイント - ポイント型回線の途中にアドレス境界を置く場合

ポイント - ポイント型回線の場合はホスト経路としてアドレス情報を管理します。したがって，本装置だけで構成されたネットワークでは次の図に示すようにポイント - ポイント型回線の途中にアドレス境界を置くこともできます。

図 12-5　ポイント - ポイント型回線の途中にアドレス境界を置く例

この図に示すように，ポイント - ポイント型接続の場合は，一つのルータを本装置 A と本装置 B とに分割し，両者の間を回線で接続したような考え方を取っています。したがって，本装置 A のインタフェース Ia にはネットワーク A 側の IP アドレス (172.17.100.1) が付けられ，本装置 B のインタフェース Ib にはネットワーク B 側の IP アドレス (172.16.200.1) が付けられます。この結果アドレス境界はポイント - ポイント型回線の途中となります。

利点

ネットワーク A とネットワーク B が別組織の場合，両者のルータをそれぞれの組織の管理下に明確に分離できるため，管理範囲が明快 (なお，回線は共用) になります。

制限事項

- 本装置間だけでできます。そのほかのルータ間では使用しないでください。
- SNMP を利用したネットワーク管理装置のネットワーク構成画面では，ポイント - ポイント型回線の両端の IP アドレスが異なるネットワークアドレスの場合，ルータ間の結線を手動で行う必要があります。

12.2.4　共用アドレスインタフェース

本装置ではポイント - ポイント型回線に専用の IP アドレスを割り当てないで，イーサネット側の IP アドレスを割り当てることができます。

利点

IP アドレスを節約できます。

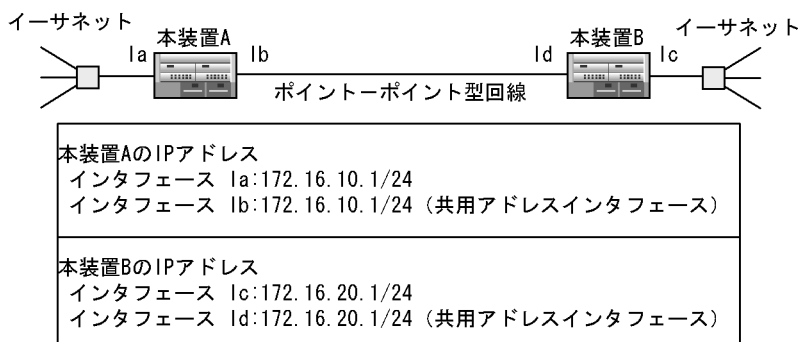
制限事項

SNMP を利用したネットワーク管理装置のネットワーク構成画面では，共用アドレスインタフェースを使用したルータ間の結線は手動で行う必要があります。

(1)　アドレス設定

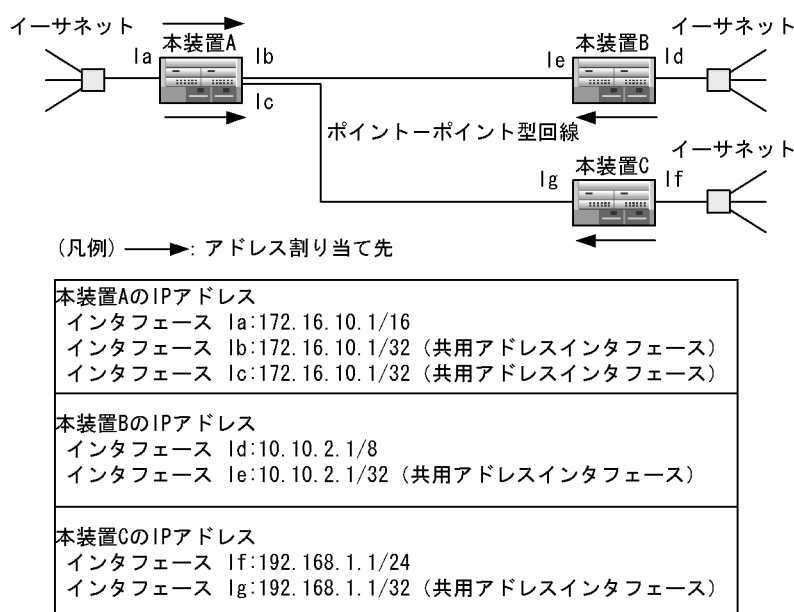
(a)　同じネットワークアドレスを持つイーサネット間接続の場合

次の図に示すように，ポイント - ポイント型回線で接続するイーサネット側に割り当てた IP アドレスのネットワークアドレス (アドレスクラスに対応したネットワークアドレス) が同じで，サブネット長も等しい場合は，お互いの共用アドレスインタフェースのサブネットマスクはイーサネット側と合わせてください。

図 12-6　共用アドレスインタフェースのアドレス設定例 1

インタフェースIaとIcのネットワークアドレス(172.16)が等しく，サブネット長も24で等しいため，インタフェースIb，Id(共用アドレスインタフェース)のサブネット長を24とする

(b) 異なるネットワークアドレスを持つイーサネット間接続の場合

異なるネットワークアドレスを持つイーサネットを接続する場合の共用アドレスインタフェースのアドレス設定例を次の図に示します。

図 12-7　共用アドレスインタフェースのアドレス設定例 2

この図では，本装置 A は一つのイーサネット側インタフェース (Ia) の IP アドレスを二つのポイント - ポイント型インタフェース (Ib，Ic) に割り当てています。この時，ポイント - ポイント型インタフェース側のサブネットマスクはイーサネット側とは異なる 32 ビットマスクとします。同様に，本装置 B と本装置 C はイーサネット側インタフェースのアドレスをポイント - ポイント型インタフェースに割り当てています。

(2) 禁止構成

● 2 台のルータ間で複数の共用アドレスインタフェースを接続しないでください。

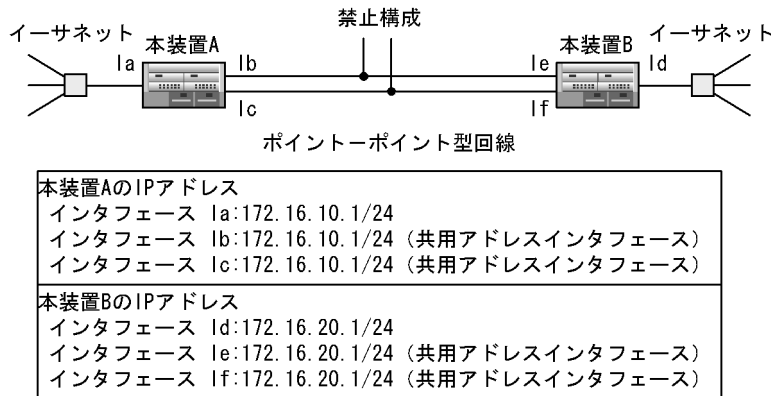
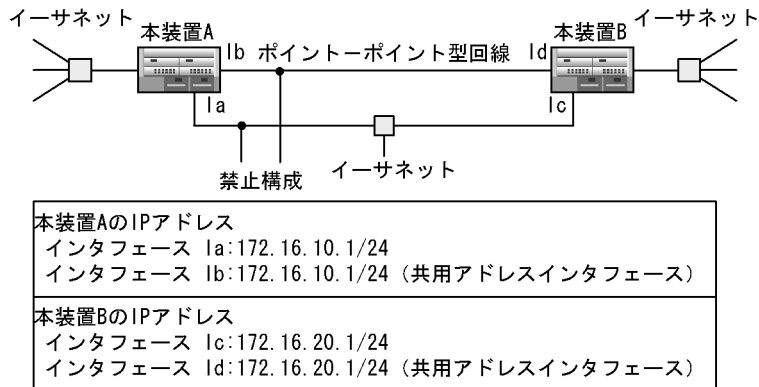
図 12-8　共用アドレスインタフェースの禁止構成例 1

● 2 台のルータ間で共用アドレスインタフェースに対応するイーサネット回線と共用アドレスインタフェースを同時に接続しないでください。

図 12-9　共用アドレスインタフェースの禁止構成例 2

12.2.5　マルチホーム・ネットワークの設計

マルチホーム接続されたルータ間で RIP-2 および ospf を使用する場合は，次の制限事項があります。

RIP-2 および ospf では送信するルーティング・パケットにマルチキャストアドレスを使用します。マルチキャストアドレスで指定されたルーティング・パケットはマルチホーム接続されたすべてのルータに対して送達されるため，ルータに不要な負荷がかかることになります。

マルチホーム接続されたルータ間で RIP-2 および ospf を使用する場合は，RIP-2 ではブロードキャスト指定 (コンフィグレーションコマンド interface(rip モード) の version 2 broadcast サブコマンド)，ospf ではノンブロードキャスト指定 (コンフィグレーションコマンド interface(ospf backbone/ospf area モード) の nonbroadcast サブコマンド) を使用してください。

12.3　経路制御 (RIP/OSPF)

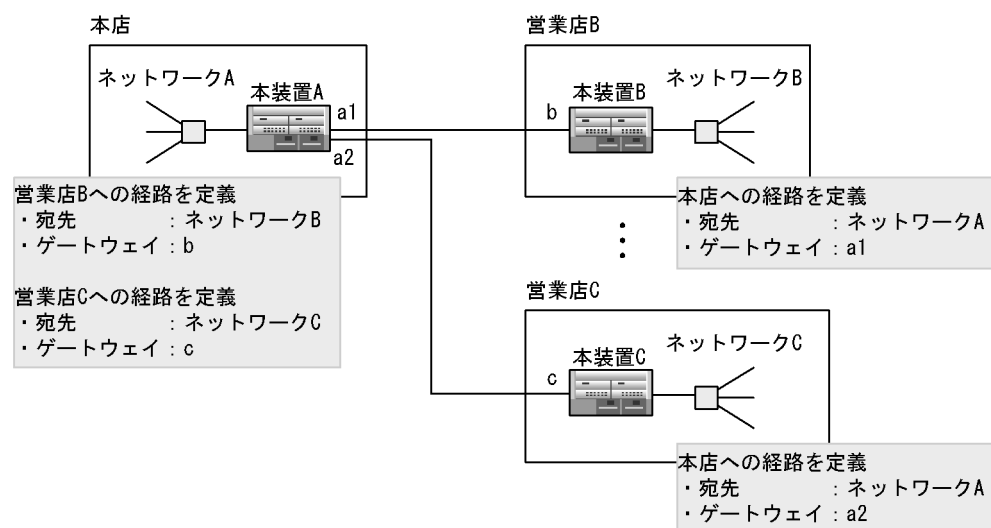
RIP および OSPF の経路制御について説明します。

12.3.1　スタティックルーティング

スタティックルーティングはコンフィグレーションで設定した経路情報 (スタティック経路) に従ってパケットを中継する機能です。

本装置のスタティック経路は，デフォルトルートを含む一つの宛先 (サブ) ネットワークまたはホストごとに，複数の中継経路 (ゲートウェイ) を設定できます。本装置は設定された複数の中継経路から適切な一つまたは複数 (コンフィグレーションコマンド options の max-paths パラメータ指定時：最大 16 パス) の経路を選択して，経路情報を生成することによってパケット中継を実現しています。

スタティックルーティングのネットワーク構成例を次の図に示します。本店からは各営業店へのスタティック経路を定義し，営業店からは本店へのスタティック経路を定義します。この設定例では営業店間の通信はできません。

図 12-10　スタティックルーティングのネットワーク構成例

(1)　スタティック経路の経路選択

コンフィグレーションで宛先ネットワークごとに指定された複数の中継経路 (ゲートウェイ) から適切な一つ，または複数 (コンフィグレーションコマンド options の max-paths パラメータ指定時) のゲートウェイを選び出し経路情報を生成します。ゲートウェイの選択は，該当するゲートウェイへ通信できる状態にあるゲートウェイの中からコンフィグレーションの定義順で選択します。

選択されたスタティック経路が使用できなくなった (インタフェースに障害が発生した) 場合，スタティック経路は設定された複数の中継経路から適切な一つ，または複数 (コンフィグレーションコマンド options の max-paths パラメータ指定時) の経路を再選択します。

(2)　スタティック経路の中継経路指定

スタティック経路では中継経路の指定方法が 3 種類あります。それぞれ，隣接ゲートウェイ，遠隔ゲートウェイ，インタフェースです。

隣接ゲートウェイ

隣接ゲートウェイは，本装置のインタフェースによって直接接続してある装置を中継経路として指定する方法です。該当するゲートウェイへの接続に使用しているインタフェースの状態によって，経路を生成・削除します。隣接ゲートウェイを指定する場合は，コンフィグレーションコマンド static の gateway サブコマンドを使用してください。

遠隔ゲートウェイ

遠隔ゲートウェイでは，本装置から直接接続していない装置を中継経路として指定できます。該当するゲートウェイへの経路の有無によって，経路を生成・削除します。遠隔ゲートウェイを使用しているスタティック経路のネクストホップは，遠隔ゲートウェイへの経路のネクストホップで置き換えられます。ただし，遠隔ゲートウェイを使用しているスタティック経路を用いて遠隔ゲートウェイを解決することはできません。

遠隔ゲートウェイを指定する場合は，コンフィグレーションコマンド static の remote-gateway サブコマンドを使用してください。

インタフェース

中継経路としてポイント - ポイント型インタフェースを指定することもできます。該当するインタフェースの状態によって，経路を生成・削除します。インタフェース指定のスタティック経路に従ってパケットを転送する場合，そのパケットを該当するインタフェースの対向装置へ転送します。インタフェースを指定する場合は，コンフィグレーションコマンド static の interface サブコマンドを使用してください。

さらに，上記指定の経路について，2 種類のサブコマンドを追加で指定できます。どちらもパケットを転送しないサブコマンドです。また，中継経路に Null インタフェースを指定した場合も，パケットを転送しません。

noinstall サブコマンド

noinstall サブコマンドを指定したスタティック経路はパケット転送に使用しません。デフォルト経路など次善の経路がある場合は，その経路に従ってパケットを転送します。noinstall サブコマンドは，広告用のスタティック経路を設定したいが，パケット転送にはこのスタティック経路を使用しないで，ほかの経路に従ってほしい場合に使用します。

reject サブコマンド

reject サブコマンドを指定したスタティック経路はリジェクト経路になります。その経路にマッチしたパケットは廃棄されます。このとき，ICMP（Unreachable）によって，送信元へパケット廃棄を通知します。reject サブコマンドは，広告用のスタティック経路を設定したいが，このスタティック経路よりも優先する経路が本装置にないパケットを廃棄したい場合に使用します。また，特定のアドレスや宛先に対してパケットを転送したくない場合にも使用します。

Null インタフェース

スタティック経路の中継経路に Null インタフェースを指定すると，結果としてパケットが廃棄されます。また，reject サブコマンドによる廃棄と違い，ICMP を送信しません。パケットを廃棄させたいが，廃棄による ICMP パケットを返したくない場合に使用します。Null インタフェースの詳細は，「11.8　Null インタフェース」を参照してください。

(3) スタティック経路の動的監視

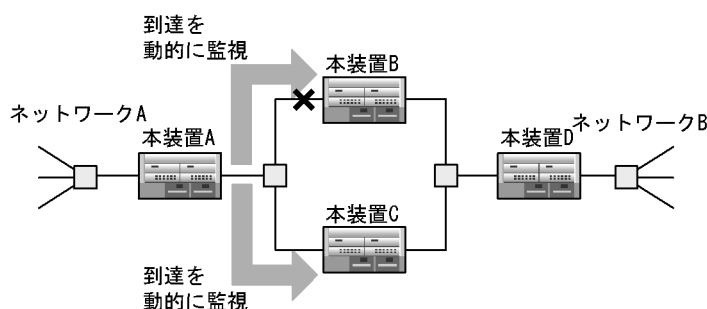
スタティック経路は，ゲートウェイと直接接続されたインタフェースの状態，またはゲートウェイへの経路の有無によって経路の生成・削除を制御します。したがって，経路が生成されている場合でも，該当するゲートウェイへの到達保証はありません。本装置では，生成されたスタティック経路のゲートウェイに対し，ICMPv4/ICMPv6 のエコー要求およびエコー応答メッセージを使用した周期的なポーリングによっ

て，到達性を動的に監視する機能 (コンフィグレーションコマンド static の poll サブコマンド) を持っています。この機能を使用することによって，「(2) スタティック経路の中継経路指定」の経路生成・削除条件に加え，該当するゲートウェイへの到達性が確保できている場合だけ，スタティック経路を生成するよう制御できます。

また，該当するゲートウェイへ到達不可能から到達可能となった場合でも，その時点で経路を生成するのではなく，一定期間該当するゲートウェイへの到達性を監視して安定性が認められた場合に経路を再生成できます。

(a) スタティック経路の動的監視による経路切り替え

スタティック経路の動的監視の例を次の図に示します。

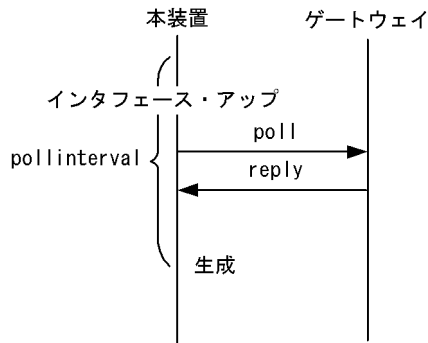
図 12-11　スタティック経路の動的監視の例

この図では，本装置 A でネットワーク B へのスタティック経路が本装置 B 経由 (優先)，本装置 C(非優先) で定義されているものとします。動的監視を行っていない状態で，本装置 A と本装置 B 間の本装置 B 側のインタフェースに障害が発生した場合，本装置 A 側のインタフェースは正常なため，本装置 B 経由のスタティック経路は削除されません。これによって，本装置 C 経由のスタティック経路への切り替えが行われず，本装置 A- ネットワーク B 間の通信が停止します。

動的監視を行っている場合，本装置 A 側のインタフェースが正常である場合でも，動的監視機能によって本装置 B への到達不可を検知し，本装置 B 経由のスタティック経路を削除します。これによって，本装置 C 経由のスタティック経路への切り替えが行われ，本装置 A- ネットワーク B 間の通信を確保できます。

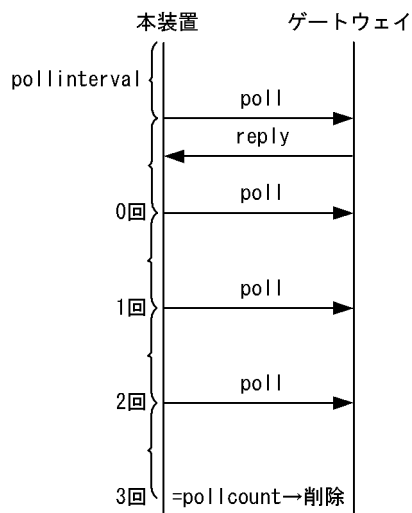
(b) スタティック経路の動的監視による経路の生成，削除および再生成タイミング

スタティック経路の動的監視による経路の生成，削除および再生成タイミングはコンフィグレーションコマンド static の pollinterval，pollcount および recovercount サブコマンドに依存します。

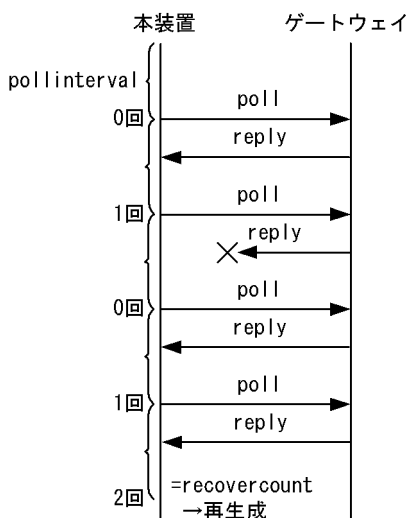
● 経路生成タイミング
インタフェースアップなどの経路生成要因を契機としてゲートウェイにポーリングします。該当するポーリングに対する応答を受信した場合，次のポーリング周期 (pollinterval) に経路を生成します。スタティック経路の動的監視による経路生成の例を次の図に示します。

図 12-12　スタティック経路の動的監視による経路生成

● 経路削除タイミング

pollinterval 周期でのポーリングに対し，pollcount 回数連続して応答がない場合に経路を削除します。pollcount=3 の場合はポーリングに対して 3 回連続して応答がない場合に経路を削除します。なお，インタフェースダウンなどの経路生成要因がなくなった場合にもポーリングを使用しない (poll サブコマンド未指定) スタティック経路と同様に，経路を削除します。スタティック経路の動的監視による経路削除の例を次の図に示します。

図 12-13　スタティック経路の動的監視による経路削除 (pollcount=3 の場合)

● 経路再生成タイミング

スタティック経路の動的監視によって削除された経路のゲートウェイへの pollinterval 周期のポーリングに対し，recovercount 回数連続して応答があった場合に経路を再生成します。recovercount=2 の場合はポーリングに対して 2 回連続して応答があった場合に経路を再生成します。スタティック経路の動的監視による経路再生成の例を次の図に示します。

図 12-14 スタティック経路の動的監視による経路再生成 (recovercount=2 の場合)

12.3.2 ダイナミックルーティング (RIP/OSPF)

本装置では RIP バージョン 1，RIP バージョン 2，OSPF バージョン 2，BGP バージョン 4，IS-IS をサポートしています。RIP については「12.4 RIP」に，OSPF については「12.5 OSPF【OP-OSPF(SB-5400S)】」に，BGP4 については「13 BGP4【OP-BGP】」に，IS-IS については「14 IS-IS【OP-ISIS】」に示します。

12.3.3 スタティックルーティングとダイナミックルーティング (RIP/OSPF) の同時動作

スタティックルーティングおよびダイナミックルーティングの各プロトコルは同時に動作できます。

(1) プリファレンス値

複数のルーティング種別が同時動作するとき，それぞれは独立した経路選択手順に従い，ある宛先アドレスへの経路情報から一つの最良の経路を選択します。その結果，ルータ内ではある宛先アドレスへの経路情報が複数存在することになります。このような場合，それぞれの経路情報のプリファレンス値が比較されて優先度の高い経路情報が有効になります。

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコル (例えば RIP) ごとに生成する経路情報のデフォルトのプリファレンス (優先度) 値をコンフィグレーションで設定できます。なお，プリファレンスは値の小さい方の優先度が高くなります。各プロトコルのプリファレンスのデフォルト値を次の表に示します。

表 12-3 プリファレンスのデフォルト値

経路	デフォルトプリファレンス値
直結経路	0(固定値)
OSPF の AS 内経路	10
IS-IS の内部経路	15
BGP4 のデフォルト経路	20
スタティック経路	60

経路	デフォルトプリファレンス値
RIP 経路	100
集約経路	130
OSPF の AS 外経路	150
IS-IS の外部経路	160
BGP4 経路	170

（2）　エキスポート機能

複数のルーティングプロトコルが同時動作するとき，各ルーティングプロトコルで広告する経路情報は同一のルーティングプロトコルで学習した経路情報および直結経路情報に限られます。異なるルーティングプロトコルから学習した経路情報は広告されません。例えば，スタティックの経路情報を RIP では広告しません。また，広告される経路情報はプリファレンス値によって選択された最も優先度の高い経路です。

本装置では，あるルーティングプロトコルの経路情報をほかのルーティングプロトコルで広告したい場合や，特定の経路情報の広告をフィルタリングしたい場合には**エキスポート機能**によって実現できます。エキスポートの設定によって広告される経路情報はプリファレンス値によって選択された最も優先度の高い経路です。

（a）　RIP-1 と RIP-2 の関係

RIP-1 と RIP-2 は同一のルーティングプロトコルです。RIP-1 と RIP-2 はお互いが学習した経路情報を広告します。

（b）　OSPF ドメインの注意事項

OSPF の各ドメインは，互いに異なるルーティングプロトコルとして動作します。このため，一つの宛先アドレスに異なる OSPF ドメインに由来する複数の OSPF AS 内経路，または OSPF AS 外経路が存在することがあります。OSPF の経路間でプリファレンス値が同じ場合には，ドメイン番号の小さい経路を優先します。OSPF の AS 外経路および AS 内経路（エリア内経路，エリア間経路）は，ドメインごとにプリファレンスのデフォルト値を変更できます。

また，同様の理由で，エキスポート機能を使用しない場合はルータ内の複数の OSPF ドメイン間で互いに経路を広告することはありません。OSPF AS 内経路や OSPF AS 外経路をほかの OSPF ドメインに AS 外経路として広告したい場合には，配布先ドメインに対してエキスポート・フィルタを定義してください。

12.3.4　経路削除保留機能

経路削除保留機能は，ルーティングプロトコルが無効にした経路を，ルーティングテーブルから一定時間削除しないようにすることで，新しく代替経路が生成されるまでの間，既存経路によってフォワーディングを維持する機能です。

経路削除保留機能については，「13.2.4　経路削除保留機能」を参照してください。

12.4 RIP

12.4.1 RIP 概説

RIP(Routing Information Protocol) は，ネットワークで接続したルータ間で使用するルーティングプロトコルです。各ルータは RIP を使用して自ルータから到達できるネットワークとそのネットワークへのホップ数 (メトリック) を通知し合うことによって経路情報を生成します。

本装置は RIP のバージョン 1 とバージョン 2 をサポートしています。バージョン 0 のメッセージを受信した場合は，破棄します。バージョン 3 以上のメッセージを受信した場合は，バージョン 2 のメッセージとして扱います。

RIP の機能を次の表に示します。

表 12-4　RIP の機能

機能	RIP
triggered update	○
ホールドダウン	○
スプリットホライズン	○
ルートタグ	△
指定ネクストホップの取り込み	○
ポイズンリバース	×
認証機能	×

(凡例)　○ : 取り扱う　△ : 一部取り扱う　× : 取り扱わない

(1) メッセージの種類

RIP で使用するメッセージの種類にはリクエストとレスポンスの 2 種類があります。ルータがほかのルータに経路情報を要求する場合にはリクエストを使用し，ほかのルータからのリクエストに応答する場合と，定期的またはトポロジ変化時に自分の経路情報をほかのルータに通知する場合にレスポンスを使用します。

(2) 運用時の処理

本装置の立ち上げ時，本装置はリクエストメッセージをすべての隣接ルータに送信し，隣接ルータが持つすべての経路情報を通知するように要求します。

運用に入ると，本装置は次の三つの要因でレスポンスを送信します。

- 隣接ルータからリクエストを受信した場合で，リクエストの内容によって自分が持つ経路情報をリクエストの送信元にレスポンスで応答します。
- 定期的に行う経路情報の通知です。本装置は 30 秒ごとに自分が持つ経路情報をすべて含むレスポンスを送信し，隣接ルータに通知します。
- 経路の変化を検出したときに行う経路情報の通知です。本装置は経路の変化を検出した場合，変化した経路に関連する経路情報を含むレスポンスを送信し，隣接ルータに通知します。

各隣接ルータが送信したレスポンスを受信し，経路の変更を検出した場合は自分が持つ経路情報を更新します。レスポンスは隣接ルータとの送信の確認にも使用します。180 秒以上レスポンスを応答しないルータに対しては通信不可能と判断し，代替ルートがあるときはルーティングテーブルをその代替ルートに更新します。代替ルートがないときはルートを削除します。

(3) ルーティングループの抑止処理

なお，本装置は中継経路のループを抑止するために**スプリットホライズン**を使用します。スプリットホライズンとは，受信した情報を受け取ったインタフェースには送信しない処理のことです。

12.4.2 経路選択アルゴリズム

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同じ宛先への経路情報が各プロトコルで生成されることによって複数存在する場合，それぞれの経路情報のプリファレンス値が比較されて優先度の最も高い経路情報が有効になります。

RIP では，自プロトコルを使用し学習した同じ宛先への広告元の異なる複数の経路情報から，経路選択の優先順位に従って一つの最良の経路を選択します。経路選択の優先順位を次の表に示します。

表 12-5　経路選択の優先順位

優先順位	内容
高	メトリック値が最も小さい経路を選択します。
↑	エージングタイムがタイマ値の 1/2 秒以内の経路を選択します (メトリック値が同じ場合)。
	ネクストホップアドレスが最も小さい経路を選択します。
↓	経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。※
低	そのほかの場合，新しく学習した経路を無視します。

注※　この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。

その後，同じ宛先への経路情報が各プロトコル (OSPF，BGP4，スタティック) で学習した経路によって複数存在する場合は，それぞれの経路情報のプリファレンス値が比較され，優先度の最も高い経路情報をルーティングテーブルに設定します。

12.4.3 RIP-1 での経路情報の広告

ルーティングプロトコルに RIP-1(RFC1058 準拠) を使用している場合には経路情報の広告に注意が必要です。一般に経路情報は次の表に示す 4 種類に分類されます。

表 12-6　経路情報の種類

経路情報の種類	定義	例
デフォルト経路情報	すべてのネットワーク宛ての経路情報	0.0.0.0 ／ 0
ナチュラルマスク経路情報	IP アドレスのクラスに対応したネットワークマスクの経路情報 (クラス A : 8 ビット) (クラス B : 16 ビット) (クラス C : 24 ビット)	172.16.0.0 ／ 16 • クラス B • ネットマスク : 16 ビット (255.255.0.0)
サブネット経路情報	特定のサブネット宛ての経路情報	172.16.10.0 ／ 24 • クラス B • ネットマスク : 24 ビット (255.255.255.0)

経路情報の種類	定義	例
ホスト経路情報	特定のホスト宛ての経路情報 (ポイント - ポイント型回線の経路情報も含みます)	172.16.10.1 ／ 32 • ネットマスク：32 ビット (255.255.255.255)

RIP-1 を使用する場合は，RIP メッセージを送信するポートのサブネットマスク値によって，広告する経路情報のエントリに制限が付きます。同一ネットワークアドレス内ですべて同一のサブネットマスクを使用する場合は問題ありません。しかし，サブネットマスクを 2 種類以上使用する場合 (可変長サブネットマスク：VLSM(Variable Length Subnet Mask)) は問題になります。VLSM となるネットワークではルーティングプロトコルに RIP-2(RFC2453 準拠) を使用する必要があります。この場合，一部で RIP-1 も併用する場合には次の表に示す RIP-1 の経路情報の広告条件に注意してください。

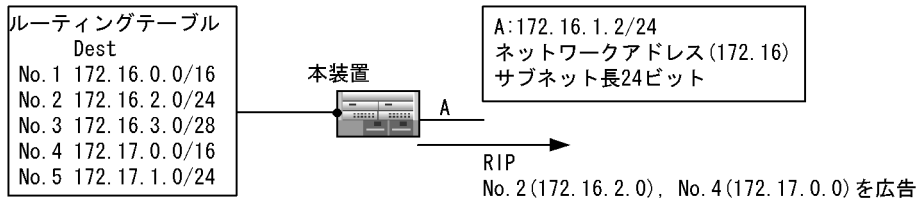
表 12-7　RIP-1 の経路情報の広告条件

広告する経路情報	広告条件	例
デフォルト経路情報	無条件に広告します。ただし，RIP 以外で学習したデフォルト経路情報はエキスポートの設定が必要です。	-
ナチュラルマスク経路情報	• ブロードキャスト型で接続している場合，本装置が保持しているナチュラルマスク経路情報とインタフェースのネットワークアドレス (アドレスクラスに対応したネットワークアドレス) が異なるとき。	「図 12-15　ブロードキャスト接続で広告する経路情報」参照
	• ポイント - ポイント型で接続している場合，本装置が保持しているナチュラルマスク経路情報と接続相手のインタフェースのネットワークアドレスが異なるとき。	「図 12-16　ポイント - ポイント接続で広告する経路情報」参照
サブネット経路情報	• ブロードキャスト型で接続している場合，本装置が保持しているサブネット経路情報のネットワークアドレス (アドレスクラスに対応したネットワークアドレス) とインタフェースのネットワークアドレスが一致し，該当するサブネット経路情報のサブネット長とインタフェースアドレスのサブネット長が一致したとき。	「図 12-15　ブロードキャスト接続で広告する経路情報」参照
	• ポイント - ポイント型で接続している場合，本装置が保持しているサブネット経路情報のネットワークアドレスと自インタフェースのネットワークアドレスおよび接続相手のインタフェースのネットワークアドレスが一致し，該当するサブネット経路情報のサブネット長と接続相手のインタフェースアドレスのサブネット長が一致したとき。	「図 12-16　ポイント - ポイント接続で広告する経路情報」参照
ホスト経路情報	本装置が保持している全ホスト経路情報のうち，無番号インタフェースを除くすべてのホスト経路情報を広告します。	「図 12-17　ホスト経路情報の広告条件」参照

(凡例)　- : 該当しない

(1)　ブロードキャスト接続のナチュラルマスク経路およびサブネットマスク経路情報の広告

ブロードキャスト接続で広告する経路情報を次の図に示します。

図 12-15　ブロードキャスト接続で広告する経路情報

●ルーティングテーブル上の各経路情報の取り扱い
No.1：インタフェースAのネットワークアドレスと一致するナチュラル・マスク経路情報なので広告されない。
No.2：インタフェースAのネットワークアドレスと一致し，サブネット長も一致するサブネット経路情報なので広告される。
No.3：インタフェースAのネットワークアドレスと一致するが，サブネット長が異なるサブネット経路情報なので広告されない。
No.4：インタフェースAのネットワークアドレスと一致しないナチュラル・マスク経路情報なので広告される。
No.5：インタフェースAのネットワークアドレスと一致しないサブネット経路情報なので広告されない。

また，この図でのブロードキャスト接続の広告条件を次の表に示します。

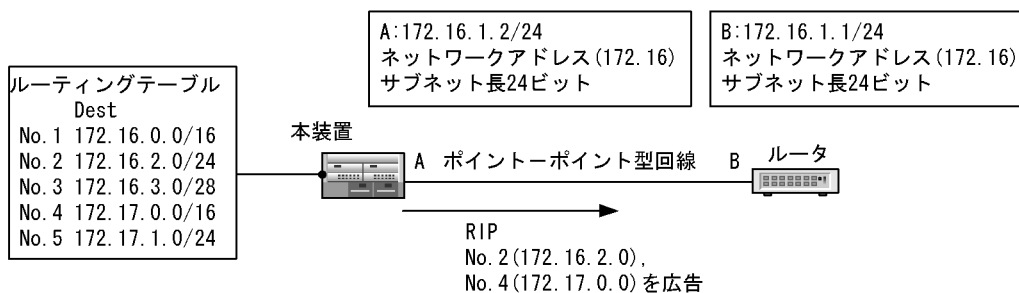
表 12-8　ブロードキャスト接続の広告条件

経路情報の種類	ルーティングテーブル上の経路情報	広告条件		広告の有無
		インタフェースＤのネットワークアドレスとの一致／不一致	インタフェースＤのサブネット長との一致／不一致	
ナチュラルマスク経路	172.16.0.0/16(No.1)	一致	-	×
	172.17.0.0/16(No.4)	不一致	-	○
サブネット経路	172.17.1.0/24(No.5)	不一致	一致	×
	172.16.2.0/24(No.2)	一致	一致	○
	172.16.3.0/28(No.3)	一致	不一致	×

(凡例)　○：広告する　×：広告しない　-：該当しない

(2)　ポイント - ポイント接続でのナチュラルマスク経路およびサブネットマスク経路情報の広告

ポイント - ポイント接続で広告する経路情報を次の図に示します。なお，この図の構成でインタフェース A，B のネットワークアドレスが異なっている場合，サブネット経路情報は広告されません。

図 12-16　ポイント - ポイント接続で広告する経路情報

●ルーティングテーブル上の各経路情報の取り扱い
No.1：インタフェースBのネットワークアドレスと一致するナチュラル・マスク経路情報なので広告されない。
No.2：インタフェースAおよびBのネットワークアドレスと一致し，サブネット長も一致するサブネット経路情報なので広告される。
No.3：インタフェースAおよびBのネットワークアドレスと一致するが，サブネット長が異なるサブネット経路情報なので広告されない。
No.4：インタフェースBのネットワークアドレスと一致しないナチュラル・マスク経路情報なので広告される。
No.5：インタフェースAおよびBのネットワークアドレスと一致しないサブネット経路情報なので広告されない。

また，ポイント - ポイント接続のナチュラルマスク経路情報の広告条件を「表 12-9　ポイント - ポイント接続のナチュラルマスク経路情報の広告条件」に，ポイント - ポイント接続のサブネット経路情報の広告条件を「表 12-10　ポイント - ポイント接続のサブネット経路情報の広告条件」に示します。

表 12-9　ポイント - ポイント接続のナチュラルマスク経路情報の広告条件

経路情報の種類	ルーティングテーブル上の経路情報	広告条件	広告の有無
		インタフェースＥのネットワークアドレスとの一致／不一致	
ナチュラルマスク経路	172.16.0.0/16(No.1)	一致	×
	172.17.0.0/16(No.4)	不一致	○

（凡例）　○：広告する　×：広告しない

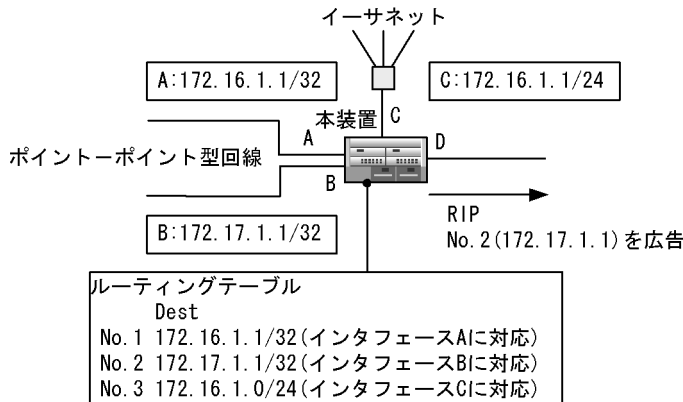
表 12-10　ポイント - ポイント接続のサブネット経路情報の広告条件

経路情報の種類	ルーティングテーブル上の経路情報	広告条件		広告の有無
		インタフェースＤおよびＥのネットワークアドレスとの一致／不一致	インタフェースＤおよびＥのサブネット長との一致／不一致	
サブネット経路	172.17.1.0/24(No.5)	不一致	一致	×
	172.16.2.0/24(No.2)	一致	一致	○
	172.16.3.0/28(No.3)	一致	不一致	×

（凡例）　○：広告する　×：広告しない

(3)　ホスト経路情報の広告

ホスト経路情報の広告条件を次の図に示します。

図 12-17　ホスト経路情報の広告条件

●ルーティングテーブル上の各経路情報の取り扱い
No.1：無番号インタフェース（インタフェースAとCのインタフェースアドレスが同じ）に関する経路情報のため広告されない。
No.2：インタフェースBに対応するホスト経路情報なので広告される。
No.3：サブネット経路情報の広告条件に従う。

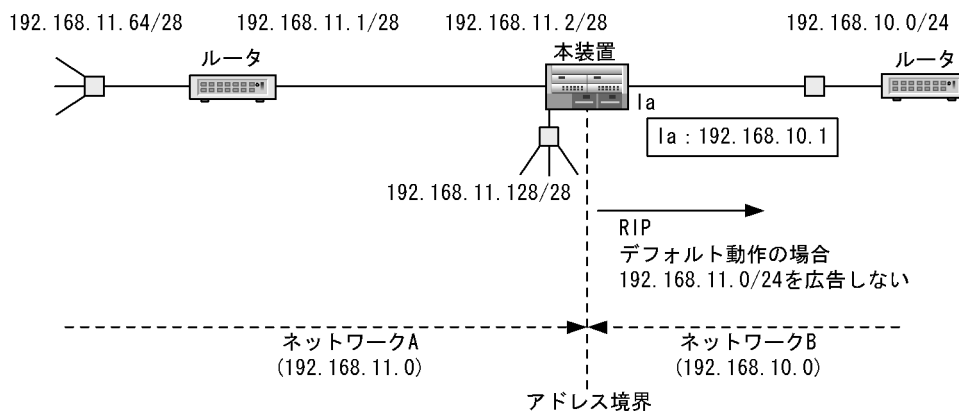
(a) IP インタフェースが一つの場合の RIP 広告について

本装置では動作できる (インタフェースがアップしており通信できる)IP インタフェースが一つの場合には RIP 広告を行いません。動作できるインタフェースが一つの場合でも RIP 広告を行わせるには，コンフィグレーションコマンド rip の broadcast サブコマンドで設定する必要があります。

直結経路を広告しない場合

本装置では，該当する装置の各インタフェースが持つ IP アドレスに対するナチュラルマスク経路情報を自動生成しません。ブロードキャスト接続ではサブネット経路情報を，ポイント - ポイント接続ではホスト経路情報を生成します。

RIP-1 ではアドレス境界をまたがる場合，サブネット経路情報は広告しないため注意が必要です。構成例を次の図に示します。

図 12-18　直結経路を広告しない構成例

注意すべき構成

- ルーティングプロトコルは RIP-1。
- 本装置上にアドレス境界を生成する。
- ブロードキャスト接続するインタフェースのサブネットマスクが，ナチュラルマスクではない。

対策 1

- コンフィグレーションで，経路集約 (サブネット経路情報およびホスト経路情報をナチュラルマスク経路情報に集約する) を設定する。
- コンフィグレーションで，エキスポート (集約経路を RIP にエキスポートする) 機能を設定する。

対策 2

- コンフィグレーションで，サブネットワーク化されたインタフェースに対応するナチュラルマスクのダイレクト経路を生成するように設定する (コンフィグレーションコマンド options の gen-class-route パラメータ)。
- 上記経路はダイレクト経路として取り扱っているので，デフォルト (エキスポートの設定なし) で広告されます。

注意事項：RIP の異なる実装

本装置ではサブネット経路をネットワーク経路に集約するためには経路集約の定義が必要であり，集約経路はアクティブ経路としてフォワーディング・テーブルに登録されます。RIP の異なる実装ではサブネット経路を自動的にネットワーク経路に集約して広告する装置もあり，通常該当する集約経路はフォワーディング・テーブルに登録されません。集約経路をフォワーディング・テーブルに登録しないような装置と互換の動作をさせる場合には経路集約のコンフィグレーションコマンド aggregate の noinstall サブコマンドで指定してください。

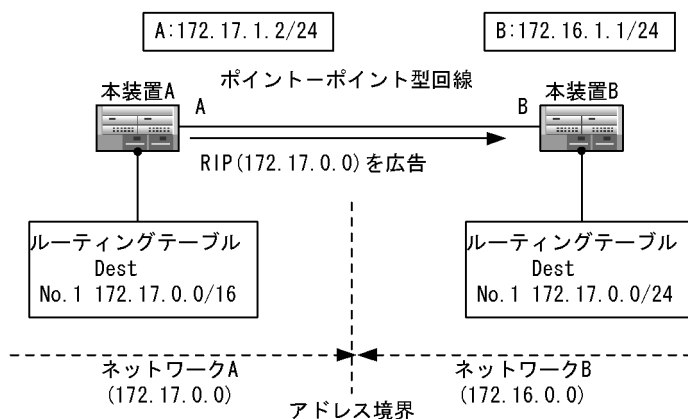
ポイント - ポイント型回線途中にアドレス境界を作る場合

禁止構成

- ルーティングプロトコルは RIP-1。
- ポイント - ポイント型回線の両端が異なるネットワークアドレスのインタフェースアドレスを持つ。(ポイント - ポイント型回線上にアドレス境界を作る。)
- マスク長はサブネットマスク。(ナチュラルマスクでもなくホストマスクでもない)

問題となる事例

ナチュラルマスク経路情報の広告で次の図に示すように，経路広告側と広告情報を受け取った側のルーティングテーブルに経路情報の不一致が生じます。

図 12-19　ポイント - ポイント接続のナチュラルマスク経路情報の不一致

12.4.4　RIP-2 の機能

RIP-2 は広告する経路情報に該当する経路のサブネットマスクを設定するため，RIP-1 のような経路広告上の制限はなく，可変長サブネットを取り扱うことができます。RIP-2 固有の機能を次に示します。なお，認証機能はサポートしていません。

(1) ルートタグ

本装置ではレスポンスメッセージで通知された経路情報のルートタグ情報が設定されている場合，ルーティングテーブルにルートタグ情報を取り込みます。本装置から通知するレスポンスメッセージの経路情報のルートタグ情報は，ルーティングテーブルの該当する経路のルートタグを設定します。なお，使用できる範囲は 1 ～ 255(10 進数) です。

また，RIP-2 ではインポート・フィルタでのルートタグ情報によるフィルタリング，およびエキスポート・フィルタ (ほかのプロトコルから RIP-2 に経路を配布する) でのルートタグ情報の変更はサポートしていません。

(2) サブネットマスク

本装置ではレスポンスメッセージで通知された経路情報のサブネットマスク情報が設定されている場合，ルーティングテーブルに該当するサブネットマスク情報を取り込みます。サブネットマスク情報が設定されていない場合，RIP-1 での経路情報受信と同様に扱います。

本装置から通知するレスポンスメッセージの経路情報のサブネットマスク情報は，ルーティングテーブルの該当する経路のサブネットマスクを設定します。

(3) ネクストホップ

本装置ではレスポンスメッセージで通知された経路情報のネクストホップ情報が設定されている場合，ルーティングテーブルに該当するネクストホップ情報を取り込みます。ネクストホップ情報が設定されていない場合，送信元のゲートウェイをネクストホップとして認識します。

本装置から通知するレスポンスメッセージの経路情報のネクストホップ情報は，通知する経路情報のネクストホップが送信先ゲートウェイと同一のネットワーク上にある場合，ルーティングテーブルの該当する経路のネクストホップを設定します。同一のネットワーク上にない場合，送信インタフェースのインタフェースアドレスを設定します。

(4) マルチキャストアドレスの使用

本装置では RIP-2 メッセージを受信しないホストでの不要な負荷を軽減するために，マルチキャストアドレスをサポートします。RIP-2 メッセージ送信時に使用するマルチキャストアドレスは 224.0.0.9 を使用します。

12.4.5 RIP による経路広告／切り替えタイミング

RIP による経路広告／切り替えのタイミングは，次の表に示す機能が関係します。

表 12-11 RIP による経路広告／切り替えのタイミング

機能	タイマ名称	タイマ値 (秒)	内容
周期的な経路情報広告	周期広告タイマ	30 (デフォルト)	自ルータが持つ経路情報を隣接ルータに周期的に通知するために使用します。
エージングタイムアウト	エージングタイマ	180 (デフォルト)	隣接ルータから通知された経路情報の周期的な通知が一定時間ない場合に，経路情報を削除するために使用します。
triggered update	-	-	自ルータの経路情報に変更があったときに定期的な広告を待たないで通知するときに使用します。
ホールドダウン	ホールドダウンタイマ	120 (デフォルト)	経路情報が削除されたことを隣接ルータに一定時間通知するために使用します。

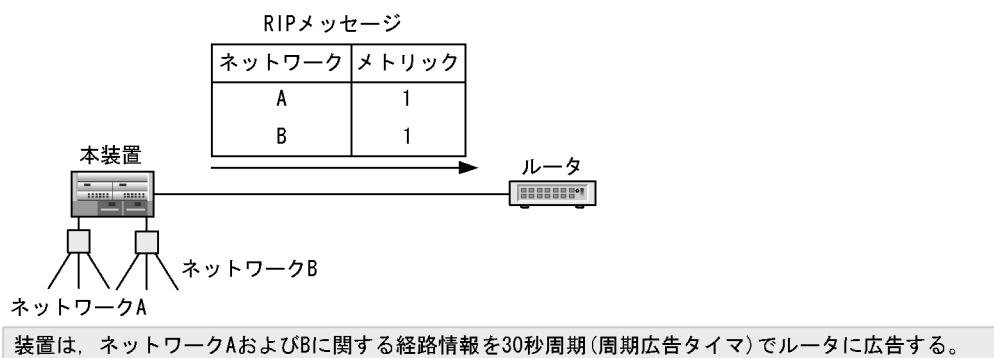
（凡例）　-：該当しない

注　周期広告タイマ，エージングタイマおよびホールドダウンタイマは，コンフィグレーションで変更できます。

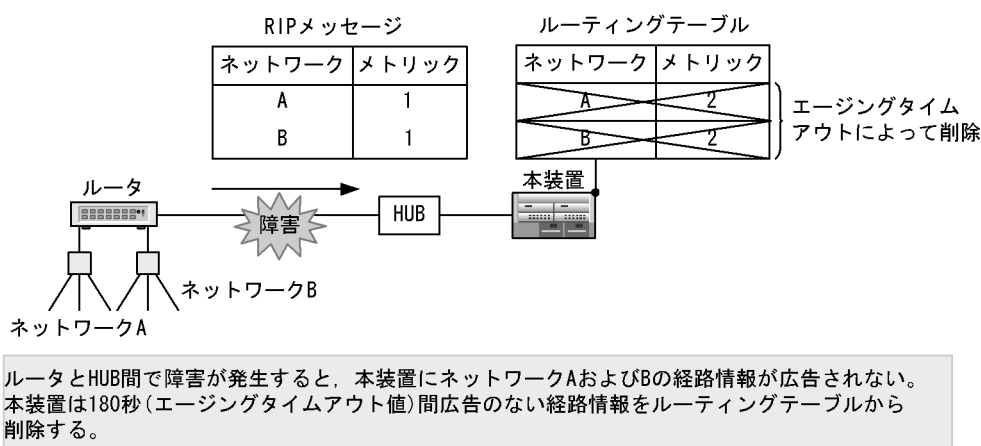
（1） 周期的な経路情報広告

RIP は自装置が持つすべての経路情報を周期的に隣接のルータに広告します。周期的な経路情報広告を次の図に示します。

図 12-20　周期的な経路情報広告

装置は，ネットワークAおよびBに関する経路情報を30秒周期（周期広告タイマ）でルータに広告する。

（2） エージングタイムアウト

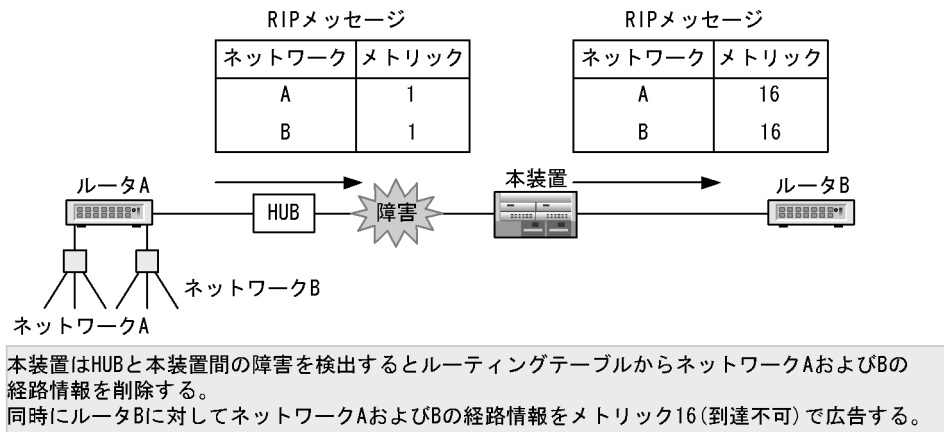
RIP は隣接から受信した経路情報が最良の経路である場合，自装置のルーティングテーブルに取り込みます。取り込んだ経路情報は**エージングタイマ**によって監視されます。エージングタイマは隣接からの周期的な広告によってリセット（クリア）します。隣接装置の障害や自装置と隣接装置間の回線障害などによって，隣接から該当する経路情報の広告が 180 秒（エージングタイムアウト値）間発生しない場合，該当する経路情報を自装置のルーティングテーブルから削除します。エージングタイムアウトによる経路情報の削除を次の図に示します。

図 12-21　エージングタイムアウトによる経路情報の削除

ルータとHUB間で障害が発生すると，本装置にネットワークAおよびBの経路情報が広告されない。
本装置は180秒（エージングタイムアウト値）間広告のない経路情報をルーティングテーブルから削除する。

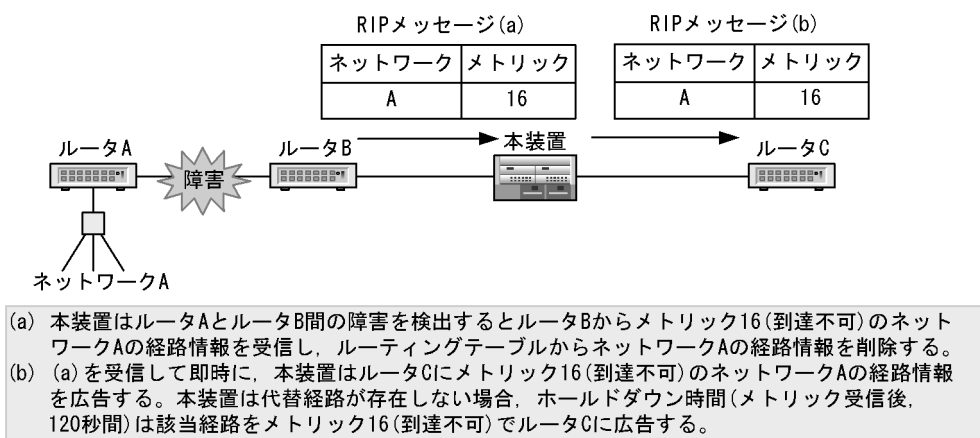
（3） triggered update

自装置の経路情報の変化を認識したときに定期的な配布周期を待たないで経路情報を配布します。triggered update による経路情報の広告を次の図に示します。

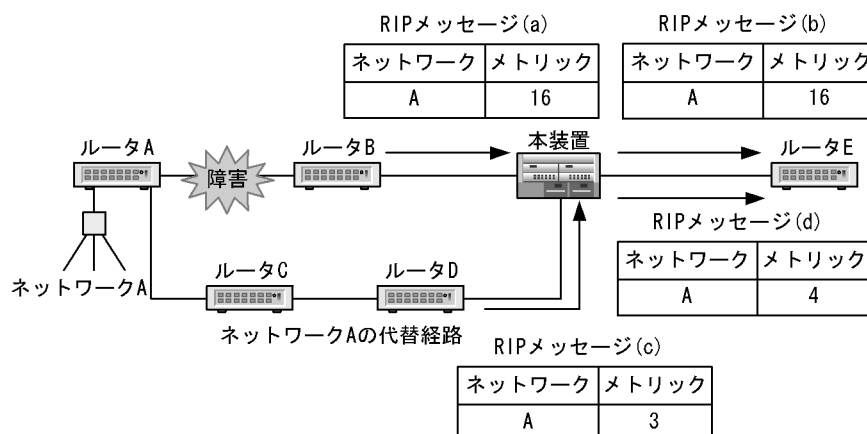
図 12-22　triggered update による経路情報の広告

本装置はHUBと本装置間の障害を検出するとルーティングテーブルからネットワークAおよびBの経路情報を削除する。
同時にルータBに対してネットワークAおよびBの経路情報をメトリック16（到達不可）で広告する。

（4） ホールドダウン

到達できる状態から到達できない状態 (メトリック 16 受信または，インタフェース障害によって該当するインタフェースから学習した経路を削除) となった経路に対して，一定時間 (120 秒：ホールドダウンタイマ) はメトリック 16(到達できない) で隣接ルータに広告します。ホールドダウンタイマは古くなったメッセージを誤って受け取ることのないように十分な時間になっています。ホールドダウンを次の図に示します。

図 12-23　ホールドダウン

(a)　本装置はルータAとルータB間の障害を検出するとルータBからメトリック16（到達不可）のネットワークAの経路情報を受信し，ルーティングテーブルからネットワークAの経路情報を削除する。
(b)　(a)を受信して即時に，本装置はルータCにメトリック16（到達不可）のネットワークAの経路情報を広告する。本装置は代替経路が存在しない場合，ホールドダウン時間（メトリック受信後，120秒間）は該当経路をメトリック16（到達不可）でルータCに広告する。

ホールドダウン期間中に，該当する宛先への新しい経路を再学習した場合は，ホールドダウンタイマを停止し，新しい経路を広告します。ホールドダウン期間中の再学習を次の図に示します。

図 12-24　ホールドダウン期間中の再学習

(a) 本装置はルータAとルータB間の障害を検出するとルータBからメトリック16(到達不可)のネットワークAの経路情報を受信し，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) 同時に本装置はルータEにメトリック16(到達不可)のネットワークAの経路情報を広告する。
(c) 本装置はルータDからの周期広告でネットワークAの経路情報を受信し，ルーティングテーブルに追加する(切り替え時間はルータDの周期広告時間による)。
(d) 本装置はホールドダウンタイマを停止し，ルータEに対してネットワークAの経路情報を広告する。

12.4.6　メッセージ送受信相手の限定

(1) 通信相手の指定

RIP では通常，ブロードキャスト型インタフェースに対するメッセージの送信は，RIP-1 ではブロードキャスト，RIP-2 ではマルチキャストを使用します。このとき，コンフィグレーションコマンド rip の targetgateways サブコマンドを指定すると，メッセージをブロードキャスト型ネットワーク上の特定の隣接ルータに対してユニキャストで送信できます。送信相手を個別に指定することで，個々の相手ごとに細かなフィルタリングを指定できるようになり，ネットワーク上に存在する RIP を受信しないホストの不要な負荷を軽減できます。

(2) 受信相手の指定

コンフィグレーションコマンド rip の trustedgateways サブコマンドを指定すると，メッセージ受信相手を限定できます。

12.4.7　高速経路切替機能

(1) 概要

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報 (第 1 優先経路と呼ぶ) と，第 1 優先経路の次に優先される経路 (第 2 優先経路と呼ぶ) をあらかじめルーティングテーブルに登録しておき，インタフェースダウンによって第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディング・テーブルに登録することによって通信停止時間の短縮を図る機能です。

高速経路切替機能の詳細については「13.2.5　高速経路切替機能」を参照してください。

(2) 第 2 優先経路の生成

コンフィグレーションコマンド options の fast-reroute パラメータおよびコンフィグレーションコマンド

rip の fast-reroute サブコマンドの gen-secondary-route パラメータ，または gen-secondary-route サブコマンドを指定することによって，異なる隣接装置から学習した同一宛先への経路情報を二つ（第 1 優先経路と第 2 優先経路）まで生成します。RIP では高速経路切替機能用に第 2 優先経路を生成する指定と，高速経路切替機能を使用せずに第 2 優先経路を生成する指定ができます。第 2 優先経路を生成する条件を次の表に示します。

表 12-12　第 2 優先経路の生成条件

条件				第 2 優先経路の生成
コンフィグレーションコマンド options の fast-reroute パラメータ	コンフィグレーションコマンド rip の fast-reroute サブコマンドの gen-secondary-route パラメータ	コンフィグレーションコマンド rip の gen-secondary-route サブコマンド	プリファレンス値	
×	-	-	-	生成しない
○	×	-	-	生成しない
○	○	-	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
○	○	-	第 1 優先経路と第 2 優先経路の値が同じ	生成する
-	-	×	-	生成しない
-	-	○	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
-	-	○	第 1 優先経路と第 2 優先経路の値が同じ	生成する

（凡例）○：コンフィグレーションあり　×：コンフィグレーションなし　-：対象外
注　コンフィグレーションコマンド options の fast-reroute パラメータとコンフィグレーションコマンド rip の gen-secondary-route サブコマンドは同時に指定できません。

第 2 優先経路の生成を指定した場合，次の表に従って同じ宛先への経路情報の優先度を決定します。

表 12-13　第 2 優先経路の登録を指定した場合の経路選択の優先順位

優先順位	内容
高	メトリック値が小さい経路を選択します。
↑	エージングタイムがタイマ値の 1/2 秒以内の経路を選択します（メトリック値が同じ場合）。
	ネクストホップアドレスが小さい経路を選択します。※1
	経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。※2
↓	今まで第 1 優先であった経路を選択します。
低	そのほかの場合，新しく学習した経路を無視します。

注
ネクストホップアドレスが同じ場合は第 1 優先経路だけ生成します。

注※ 1

第 2 優先経路が登録されている状態で新経路を学習した場合，この条件は適用されません。

注※ 2

この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。

12.4.8　RIP 使用時の注意事項

本装置は RFC1058(RIP-1)，RFC2453(RIP-2) に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 12-14　RFC との差分

RFC			本装置
RFC1058(RIP-1)	サブネットの広告	サブネット化されたネットワークと接続している境界ゲートウェイは，ほかの隣接ゲートウェイに対して全体のネットワーク経路だけを広告します。	本装置ではサブネットワーク経路からネットワーク経路を自動的に生成しません。サブネットワーク経路からネットワーク経路を生成したい場合は，経路集約機能を使用する必要があります。
		一般に全体のネットワークのメトリックは，サブネットの中で一番小さいメトリックが採用されます。	本装置ではサブネットワーク経路からネットワーク経路を自動的に生成しません。サブネットワーク経路からネットワーク経路を生成したい場合は，経路集約機能を使用する必要があります。集約経路のメトリック値は RIP のデフォルト・メトリック値またはエキスポート・フィルタで指定したメトリック値を使用します。
		境界ゲートウェイは直接接続されたネットワークにあるホスト経路をほかのネットワークに対して広告してはなりません。	本装置では直接接続されたネットワークにあるホスト経路を，ルーティングテーブルに追加および広告します。
	レスポンス受信	すでに存在するネットワーク経路またはサブネットワーク経路に含まれるホスト経路は追加しないことが望ましいです。	本装置ではレスポンスによってホスト経路を受信した場合，ルーティングテーブルに追加します。
RFC2453(RIP-2)	認証	平文パスワードをサポートします。	本装置では認証機能はサポートしていません。
	ルートタグ	ルートタグは，RIP 内経路と RIP 外経路を切り分けるために使用します。	本装置ではルートタグによるフィルタリングはサポートしていません。
		RIP 以外のプロトコルをサポートするルータは異なるプロトコルからインポートされた経路のルートタグを変更できるようにすべきです。	本装置ではほかのプロトコルから RIP に広告する経路のルートタグは変更できません。
	互換性	RIP-2 ルータが RIP-1 のリクエストを受信した場合，RIP-1 のレスポンスで応答すべきです。RIP-2 だけを送信するように設定されている場合，レスポンスは送信すべきではありません。	本装置は RIP-2 インタフェースでは RIP-2 のレスポンスだけを送信します。このため，RIP-1 のリクエストを受信した場合，リクエストに対するレスポンスは送信しません。
		受信制御スイッチ（RIP-1 だけを許す，RIP-2 だけを許す，両方許す，受信を受け付けない）を持つべきです。これらはインタフェース単位に行います。	本装置ではインタフェース単位で RIP の受信を制御できますが，RIP-1，RIP-2 を区別した受信制御はできません。

12.5 OSPF【OP-OSPF(SB-5400S)】

12.5.1 OSPF 概説

OSPF(Open Shortest Path First) は，ルータ間の接続の状態から構成されるトポロジと，Dijkstra アルゴリズムによる最短経路計算に基づくルーティングプロトコルです。

(1) OSPF の特長

OSPF は，通常一つの AS 内で経路を決定するときに使用します。OSPF では，AS 内のすべての接続状態から構成するトポロジのデータベースが各ルータにあり，このデータベースに基づいて最短経路を計算します。このため，OSPF は RIP と比較して，次に示す特長があります。

- 経路情報トラフィックの削減
  OSPF では，ルータ間の接続状態が変化したときだけ，接続状態の情報を他ルータに通知します。このため，OSPF は RIP のように定期的にすべての経路情報を通知するルーティングプロトコルと比較して，ルーティングプロトコルが占有するトラフィックが小さくなります。なお，OSPF では 30 分周期で，自ルータの接続状態の情報だけを他ルータに通知します。
- ルーティングループの抑止
  OSPF を使用しているすべてのルータは，同じデータから成るデータベースを保持しています。各ルータは，共通のデータに基づいて経路を選択します。したがって，RIP のようなルーティングループ (中継経路の循環) は発生しません。
- コストに基づく経路選択
  OSPF では，宛先に到達できる経路が複数存在する場合，宛先までの経路上のコストの合計が最も小さい経路を選択します。これによって，RIP と異なり経路へのコストを柔軟に設定できるため，中継段数に関係なく望ましい経路を選択できます。
- 大規模なネットワークの運用
  OSPF では，コストの合計が 16,777,214 以内の経路を扱えます。このため，メトリックが 1 〜 15 までの範囲である RIP と比較して，より大規模で経由ルータ数の多い経路が存在するネットワークの運用に適しています。
- 可変長サブネット
  OSPF は，経路情報にサブネットマスクを含むため，RIP-1 とは異なり，サブネット分割してあるネットワークを宛先として取り扱えます。

使用プロトコルの選択についての注意事項

RIP-2 でも，RIP-1 とは異なり，サブネットマスクの情報を含めることによって，サブネット分割したネットワークを宛先として扱えます。単にサブネットを扱うことが目的で，すべてのルータが RIP-2 を使用可能なら，RIP-2 をお勧めします。

(2) OSPF の機能

OSPF の機能を次の表に示します。

表 12-15　OSPF の機能

機能	OSPF
ポイント - ポイント型インタフェースのアドレス広告	相手側アドレスを指定コストで広告※1
AS 外経路のフォワーディングアドレス	○
NSSA	○

機能	OSPF
認証	○
非ブロードキャスト (NBMA) ネットワーク	○
イコールコストマルチパス	○
仮想リンク	○
マルチバックボーン	○
グレースフル・リスタート	○※ 2

(凡例) ○：取り扱う

注※ 1

コンフィグレーションコマンド options の gen-prefix-route パラメータを指定した場合，マスク長が 32 ではないポイント - ポイント型インタフェースについてはネットワーク経路を指定コストで広告します。このとき相手側アドレスは広告しません。

注※ 2

SB-5400S ではヘルパー機能だけサポートします。

12.5.2 経路選択アルゴリズム

OSPF では，経路選択のアルゴリズムとして，SPF(Shortest Path First) アルゴリズムを使用します。

各ルータには，OSPF が動作しているすべてのルータと，ルータ - ルータ間およびルータ - ネットワーク間のすべての接続から成るデータベースがあります。このデータベースから，ルータおよびネットワークを頂点とし，ルータ - ルータ間およびルータ - ネットワーク間の接続を辺とするトポロジを構成します。このトポロジに SPF アルゴリズムを適用して，最短経路木を生成し，これを基に各頂点およびアドレスへの経路を決定します。

(1) SPF アルゴリズムの適用例

ネットワーク構成の例を次の図に示します。

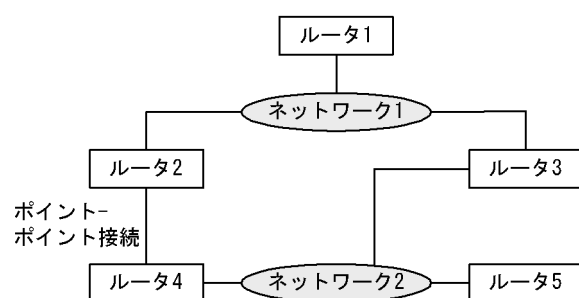
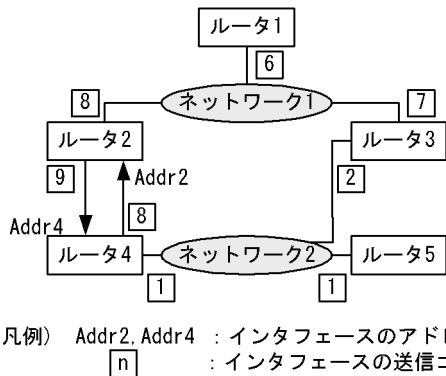
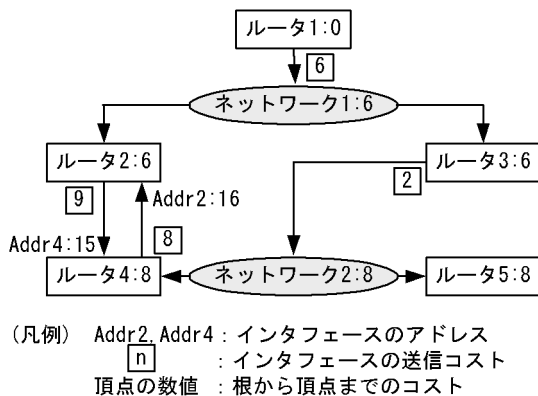
図 12-25　ネットワーク構成例

この図のネットワーク上で OSPF を使用した場合のトポロジと，頂点間のコストの設定例を次の図に示します。コスト値は，パケット送信方向によって異なってもかまいません。

図 12-26　トポロジとコストの設定例

この図のルータ 2- ルータ 4 間のポイント - ポイント型接続では，ルータ 2 からルータ 4 へはコスト 9，ルータ 4 からルータ 2 へはコスト 8 となっています。ルータ - ネットワーク間の接続では，ルータからネットワークへの接続だけにコストを設定できます。ネットワークからルータへのコストは常に 0 です。

「図 12-26　トポロジとコストの設定例」のトポロジを基に，ルータ 1 を根として生成した最短経路木を次の図に示します。ある宛先へのコストは，経路が経由する各インタフェースの送信コストの合計となります。例えば，ルータ 1 からネットワーク 2 宛ての経路のコストは，6(ルータ 1- ネットワーク 1)+0(ネットワーク 1- ルータ 3)+2(ルータ 3- ネットワーク 2)=8 となります。

図 12-27　ルータ 1 を根とする最短木

OSPF では，コストを基に最適な経路を選択します。ある構成で適切ではない経路を選択してしまう場合には，望ましくないネットワークのインタフェースのコストを上げるか，より望ましいネットワークのインタフェースのコストを下げることによって，適切な経路を指示できます。このときコストが小さ過ぎると，コストは 1 未満にできないため，このインタフェースを除く全ルータのインタフェースにかかるコストを上げなければならないことがあります。大規模なネットワークでは，将来最適化するときに任意のインタフェースのコストを減らせるように，インタフェースのコストをあまり小さく設定しないことをお勧めします。

(a)　ルータ ID，ネットワークアドレスについての注意事項

OSPF では，ネットワークのトポロジを構築するに当たり，ルータの識別にルータ ID を，ネットワークの識別にネットワークアドレスを使用します。したがって，ネットワークの設計時に次に示すように不正がある場合には，正確なトポロジを構築できません。

- 異なるルータに同じ値のルータ ID を定義した場合

- 異なるネットワークに同一ネットワークアドレスを割り当てた場合

これらの不正がある場合，不正確なトポロジに基づいてネットワーク設計することになり，正確な経路選択ができなくなります。ルータ ID の決定方法として，次の方法をお勧めします。

ルータ ID の決定方法

各ルータのルータ ID の決定に当たり，該当するルータにある OSPF が動作しているインタフェースに割り当ててある IP アドレスの中からどれか一つを選択して，これをルータ ID として使用してください。ルータ ID は，基本的には任意の 32 ビットの数値ですが，この方法を使用することで OSPF ネットワーク設計時のミスなどによるルータ ID の重複を防ぐことができます。

(b) 経路選択についての注意事項

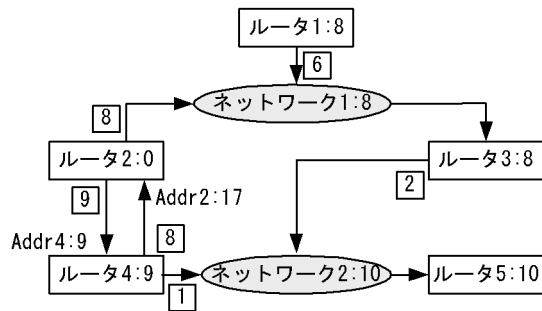
OSPF では，自ルータにあるインタフェースのアドレスは，そのインタフェースからつながっている辺の対向側の頂点 (ポイント - ポイント型インタフェースでは対向するルータ，ブロードキャスト型インタフェースではインタフェースがつながっている頂点であるネットワーク) に所属しています。このために，条件に応じて，次のような状態になることがあります。

1. 自ルータにあるインタフェースのアドレス宛ての経路は，必ず対向側の頂点を経由します。このため，例えば「図 12-25　ネットワーク構成例」のルータ 1 からルータ 2 のインタフェースのアドレスである Addr2 宛ての経路は，ルータ 1- ネットワーク 1- ルータ 3- ネットワーク 2- ルータ 4-Addr2 になります。この場合，コストは 6 (ルータ 1- ネットワーク 1)+ 0(ネットワーク 1- ルータ 3)+2(ルータ 3- ネットワーク 2)+0(ネットワーク 2- ルータ 4)+ 8(ルータ 4-Addr2)=16 になります。
2. 自ルータのポイント - ポイント型インタフェースが動作状態になっていない場合，このインタフェースの対向側ルータのインタフェースのアドレスが所属するものが存在しないため，このアドレス宛ての経路情報を生成しないことがあります。
3. 自ルータのポイント - ポイント型インタフェースが，動作状態にあるものの回線障害などの理由によって対向するルータへ送信できない場合，対向側のルータのインタフェースのアドレス宛ての経路は，自ルータを経由します。このため，対向するルータのインタフェースのアドレス宛てに通信はできない場合があります。

自ルータのブロードキャスト型インタフェースが動作状態にないか，動作状態にあるものの Hub の故障などによって同じネットワークへ接続しているほかのルータと通信できない場合，このインタフェースのアドレスに対する経路に，同じネットワークに接続しているが通信できないほかのルータ経由の経路が選択されることによって，通信できないことがあります。

(2) イコールコストマルチパス

ルータ 2 を根として生成した最短経路木を次の図に示します。

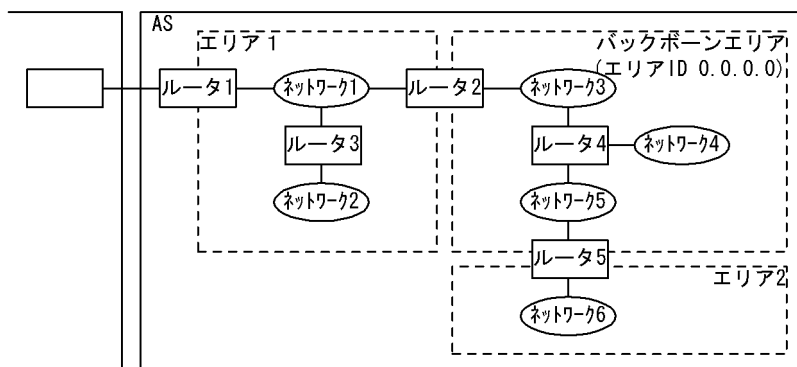
図 12-28　ルータ 2 を根とする最短木

ネットワーク 2 またはルータ 5 を宛先とした場合，ネットワーク 1 経由の経路とルータ 4 経由の経路については コストが同じになります。OSPF では，ある 2 点間に最短コストの経路が複数存在する場合，この複数の経路をイコールコストマルチパスと呼びます。

OSPF では，自ルータからある宛先についてイコールコストマルチパスが存在し，次の転送先ルータが複数ある場合，その宛先へのパケットの転送を複数のネクストホップへ分散することによって，トラフィックを分散してもよいことになっています。

本装置では，コンフィグレーションコマンド ospf の multipath サブコマンドを定義することによって，複数のネクストホップを生成できます。この複数のネクストホップ (マルチパス) 数は，コンフィグレーションコマンド options の max-paths パラメータに従います。multipath サブコマンドを定義しなかった場合，最も小さいネクストホップアドレスを選択します。

12.5.3　エリア分割

OSPF では，ルーティングに必要なトラフィックと，経路選択に使用するアルゴリズムの処理に必要な時間を削減するために，AS を複数のエリアに分割できます。エリア分割を使用した OSPF ネットワークトポロジの例を次の図に示します。

図 12-29　エリア分割を使用した OSPF ネットワークトポロジの例

あるエリア内の接続状態の情報は，ほかのエリアには通知されません。また，ルータには，接続していないエリアの接続状態の情報はありません。

(1) バックボーン

エリア ID が 0.0.0.0 であるエリアをバックボーンと呼びます。AS が複数のエリアに分割されている場合，バックボーンには特別な役割があります。AS を複数のエリアに分割する場合には，エリアのどれか一つをバックボーンエリアとして定義する必要があります。ただし，一つの AS にバックボーンを二つ以上ある構成にしないでください。そのような構成の場合，情報がそれぞれのバックボーンに分散されるため，到達不能である経路が発生したり，最適な経路を選択しなかったりすることがあります。

(2) エリアボーダルータ

「図 12-29　エリア分割を使用した OSPF ネットワークトポロジの例」のルータ 2 やルータ 5 のように，複数のエリアに所属しているルータを，エリアボーダルータと呼びます。エリアボーダルータでは，所属しているすべてのエリアについて，それぞれ別個に SPF アルゴリズムに基づいて経路選択を行います。なお，エリアボーダルータは，バックボーンを通じてエリア間の経路情報の交換を行うため，必ずバックボーンに所属する必要があります。

(a) エリア分割についての注意事項

エリア分割を行うと，ルータや経路情報トラフィックの負荷が減る一方で，OSPF のアルゴリズムが複雑になります。特に，障害に対して適切な動作をする構成が困難になります。ルータやネットワークの負荷に問題がない場合は，エリア分割を行わないことをお勧めします。

(b) エリアボーダルータについての注意事項

- エリアボーダルータでは，所属しているエリアの数だけ，SPF アルゴリズムを動作させます。エリアボーダルータには，あるエリアのトポロジ情報を要約し，ほかのエリアへ通知する機能があります。このため，所属するエリアの数が多くなるとエリアボーダルータの負荷が高くなります。このため，エリアボーダルータにあまり多くのエリアを所属させないようなネットワーク構成にすることをお勧めします。
- あるエリアにエリアボーダルータが一つしかない場合，このエリアボーダルータに障害が発生するとバックボーンから切り放され，ほかのエリアとの接続性が失われます。重要な機能を提供するサーバや重要な接続のある AS 境界ルータの存在するエリアには，複数のエリアボーダルータを配置し，エリアボーダルータの配置に対して十分な迂回路が存在するように，ネットワークを構築することをお勧めします。
- インタフェースおよび装置アドレスを同時に複数のエリアの OSPF インタフェースとなる構成にしないでください。本装置に接続している各インタフェースおよび装置アドレスは，それぞれ一つのエリアにだけ所属できます。複数のエリアに OSPF インタフェースとして定義した場合，対象インタフェースおよび装置アドレスは，どのエリアでも OSPF インタフェースとして動作しなくなります。

(3) スタブエリア

バックボーンではなく，AS 境界ルータが存在しないエリアをスタブエリアとして定義 (コンフィグレーションコマンド area(ospf モード) の stub サブコマンドで指定) できます。

エリアボーダルータは，スタブエリアとして定義したエリアに AS 外経路を導入しません。このため，スタブエリア内では経路情報を減らし，ルータの情報の交換や経路選択の負荷を減らすことができます。

AS 外経路の代わりとして，スタブエリアにデフォルトルートを導入するようにエリアボーダルータを設定 (コンフィグレーションコマンド area(ospf モード) の stub cost サブコマンドで指定) できます。この設定によって，スタブエリア内の AS 外経路の扱いについては，デフォルトルートへのコストとエリアボーダルータまでのコストの合計に基づいて，経路を選択します。ただし，デフォルトルートに基づいて経路が選択されるため，スタブエリア内では，AS 外経路について比較的遠い経路を選択することがあります。

(4) NSSA

バックボーンでないエリアを，NSSA として定義 (コンフィグレーションコマンド area(ospf モード) の nssa サブコマンドで指定) できます。

エリアボーダルータは，NSSA として定義したエリアへ，ほかのエリアから学習した AS 外経路を広告しません。このため，NSSA 内では経路情報を減らし，ルータの情報の交換や経路選択の負荷を減らすことができます。ただし，エリアボーダルータは，NSSA 内の AS 外経路を NSSA ではないエリアへ広告します (AS 外経路変換機能)。

他エリア内の AS 外経路の代わりとして，NSSA にデフォルトルートを導入するように，エリアボーダルータを設定 (コンフィグレーションコマンド area(ospf モード) の nssa cost サブコマンドで指定) できます。この設定によって，NSSA 内にデフォルトルートを AS 外経路として広告します。ただし，エリアボーダルータはこの経路を学習しません。また，NSSA 内にデフォルトルートを広告するルータが複数存在する場合，AS 外経路として優先度の高い経路を選択します。

(5) エリア分割した場合の経路制御

エリアボーダルータは，バックボーンを除くすべての所属しているエリアの経路情報を要約した上で，バックボーンに所属するすべてのルータへ通知します。また，バックボーンの経路情報の要約と，バックボーンに流れている要約されたほかのエリアの経路情報を，バックボーン以外の接続しているエリアのルータへ通知します。

あるルータが，あるアドレスについて，要約された経路情報を基に経路を決定した場合，このアドレス宛ての経路は要約された経路情報の通知元であるエリアボーダルータを経由します。このため，異なるエリア間を結ぶ経路は必ずバックボーンを経由します。

(6) エリアボーダルータでの経路の要約

エリアボーダルータでは，あるエリアの経路情報をほかのエリアに広告するに当たってルータやネットワーク間の接続状態と接続のコストによるトポロジ情報を，エリアボーダルータからルータやネットワークへのコストに要約します。

経路の集約および抑制とエリア外への要約を次の表に示します。

表 12-16 経路の集約および抑制とエリア外への要約

エリア内のネットワークアドレス	集約および抑制の設定	エリア外へ通知する要約
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24	なし	10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24	10.0.0.0/23 10.0.2.0/24	10.0.0.0/23 10.0.2.0/24 10.0.3.0/24
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24 192.168.3.0/26 192.168.3.64/26 192.168.3.128/26	10.0.0.0/8 (抑制) 192.168.3.0/24	192.168.3.0/24

エリアボーダルータでのエリア内のトポロジ情報を要約するに当たり，アドレスの範囲を定義することによって，その範囲に含まれる経路情報を一つに集約できます。アドレスの範囲の指定には，マスク付のア

ドレスを使用します (コンフィグレーションコマンド area(ospf モード) の networks サブコマンドで指定)。

集約する範囲を定義すると，エリア内にマスク付アドレスの範囲に含まれるネットワークが一つでもあった場合，範囲に含まれるすべてのネットワークをこのマスク付アドレスを宛先とする経路情報へ集約し，ほかのエリアへ通知します。範囲に含まれる各ネットワークは，このエリアボーダルータからほかのエリアへは通知されません。このとき，集約した経路情報のコストには範囲に含まれるネットワーク中の最も大きなコストを使用します。

また，このマスク付アドレスの範囲に含まれるネットワークの広告を抑制 (コンフィグレーションコマンド area(ospf モード) の networks サブコマンドで restrict を指定) できます。この場合，範囲内の各ネットワークをほかのエリアへは通知しない上に，マスク付アドレスに集約した経路もほかのエリアへは通知しません。この結果，ほかのエリアからはこのエリアボーダルータ経由で指定した範囲に含まれるアドレスへの経路は存在しないように見えます。

集約および抑止するアドレスの範囲は，一つのエリアについて複数定義できます。また，エリア内にどの定義の範囲にも含まれないアドレスを使用しているルータやネットワークが存在してもかまいません。ただし，ネットワークを構成するに当たり，トポロジと合ったアドレスを割り当てた上で，トポロジに応じた範囲を使用して集約を定義すると，選択する経路の適切さを損なわないで，効率的に OSPF の経路情報トラフィックを削減できます。

(7) 仮想リンク

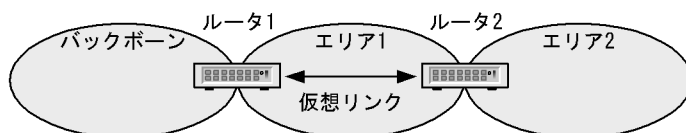
OSPF では，スタブエリア，または NSSA として定義しておらず，バックボーンでもないエリア上のある二つのエリアボーダルータで，このエリア上の二つのルータ間の経路をポイント - ポイント型回線と仮想することによって，バックボーンのインタフェースとして使用できます。この仮想の回線のことを**仮想リンク**と呼びます。仮想リンクの実際の経路があるエリアのことを，仮想リンクの通過エリアと呼びます。

仮想リンクの使い方として，次に示す三つの例を挙げます。

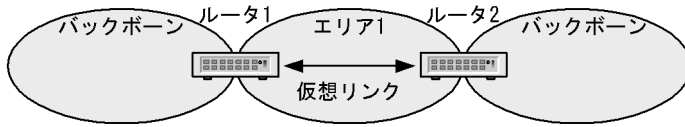
- バックボーンに物理的に接続していないエリアの仮想接続
- 複数のバックボーンの結合
- バックボーンの障害による分断に対する経路の予備

(a) バックボーンに物理的に接続していないエリアの仮想接続

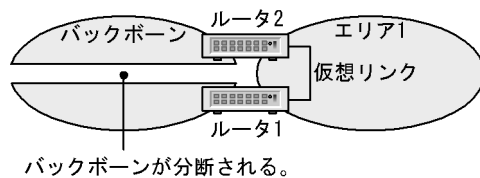
次の図で，エリア 2 はバックボーンに接続していません。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義することによって，ルータ 2 はバックボーンに接続するエリアボーダルータとなり，エリア 2 をバックボーンに接続していると見なせるようになります。

図 12-30　エリアのバックボーンへの接続

(b) 複数のバックボーンの結合

次の図では，AS 内にバックボーンであるエリアが二つ存在します。この状態では，バックボーンの分断による経路到達不能などの障害が発生することがあります。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義することによって，バックボーンが結合されることになり，この障害を回避できます。

図 12-31　バックボーン間の接続

(c) バックボーンの障害による分断に対する経路の予備

次の図では，バックボーンでネットワークの障害が発生し，ルータ 1 とルータ 2 の間の接続が切断された場合，バックボーンが分断されます。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義すると，これがバックボーンの分断に対する予備の経路（バックボーンでのルータ 1-ルータ 2 のコストと比較して，仮想リンクのコストが十分に小さい場合には，主な経路）になります。

図 12-32　バックボーン分断に対する予備経路

(d) 仮想リンクについての注意事項

仮想リンクを設定および運用するに当たって，次の注意事項に留意してください。

- 仮想リンクは，仮想リンクの両端のルータで共に設定する必要があります。
- 仮想リンクのコストは，通過エリアでの仮想リンクの両端のルータ間の経路コストになります。
- 通過エリアで，仮想リンクの両端のルータ間の経路がイコールコストマルチパスの場合，一般のトラフィックと仮想リンク上の経路情報トラフィックでは，経路が異なることがあります。
- 仮想リンク上の Hello パケットの送信間隔 (hellointerval) は，通過エリア上での仮想リンクの両端ルータ間の経路を構成する各ネットワーク上の，各インタフェースに設定してある Hello パケットの送信間隔のどれよりも長くする必要があります。この値をどれよりも短く設定した場合，通過エリア内の経路上のネットワークの障害にあたって，通過エリア内の代替経路への交替に基づいて仮想リンクが使用する経路が交替するよりも先に，仮想リンクが切断することがあります。
- 仮想リンク上の OSPF パケットの再送間隔 (retransmitinterval) は，仮想リンクの両端ルータ間をパケットが往復するのに必要な時間よりも十分に長く設定する必要があります。ただし，あまり長過ぎる値を設定すると，混雑しているネットワーク上での仮想リンクの運用時に仮想リンク上での経路情報の交換に障害が発生することがあります。

12.5.4　ルータ間の接続の検出

OSPF が動作しているルータは，ルータ間の接続性を検出するため，インタフェースごとに Hello パケットを送信します。Hello パケットを他ルータから受信することによって，ルータ間で OSPF が動作していることを認識します。

(1) ルータ間接続条件

ブロードキャスト型とポイント - ポイント型とに関係なく，ルータ間を直接接続するネットワークのそれぞれについて，接続するルータのインタフェースでの OSPF の定義は，次に示す項目が一致している必要があります。これが一致していないルータ間では，OSPF 上は，接続していないことになります。

（a） インタフェースアドレス

ブロードキャスト型ネットワークでは，同一ネットワークへ接続しているすべてのルータのインタフェースは，IP ネットワークアドレスとマスクが同じである必要があります。

（b） 認証の方式と認証の鍵

OSPF では，接続しているルータからの経路情報が正しくそのルータからのものかどうかを検証するために，認証を使用できます。認証を使用する場合は，同一ネットワークへ接続しているすべてのルータの，このネットワークへのインタフェースに定義した認証方式と鍵が一致している必要があります。認証については「12.5.6　認証」を参照してください。

（c） エリア ID

ルータ間の直接接続では，両ルータのインタフェースに定義したエリアが一致している必要があります。

（d） HelloInterval と RouterDeadInterval

OSPF では，直接接続しているルータに自ルータを検出させるために，Hello パケットを送信します。HelloInterval は Hello パケットの送信間隔，RouterDeadInterval は，あるルータからの Hello パケットを受信できないことを理由にそのルータとの接続が切れたと判断するまでの時間です。検出と切断を適切に判断するためには，直接接続しているルータのインタフェースに定義した，この二つの値が一致している必要があります。

（e） エリアの定義

スタブエリアと NSSA，そのどちらでもないエリアとでは，エリアに通知される情報が異なります。このため，OSPF が二つのルータを直接接続していると判断するには，インタフェースが所属しているエリアのスタブについての定義が一致している必要があります。

（f） OSPF を使用するインタフェースの設定についての注意事項

OSPF では，インタフェースに定義してある送信時パケットの最大長 (MTU) と同じ長さのパケットを送信する場合があります。ここで，受信側のインタフェースに定義してある受信時パケットの最大長 (MRU：特に記述がなければ，MTU と同一) よりも長い場合，通常のトラフィックでは顕在化しないルータ間の相互通信不可能の問題が発生する場合があります。

このため，OSPF を使用する場合は，特にすべてのネットワークおよびネットワークに接続しているすべてのルータのインタフェースについて，MTU が他のすべてのインタフェースの MRU 以下に定義してあることの確認をお勧めします。

（2） ブロードキャスト型ネットワークと指定ルータ

ブロードキャスト型ネットワークでは，トポロジ上の頂点であるネットワークとネットワークに直接接続しているルータ間の接続情報を管理するために，指定ルータ (Designated Router) とバックアップ指定ルータを選択します。指定ルータの障害時には，ネットワークの接続情報の管理ルータを速やかに移行するために，バックアップ指定ルータが指定ルータになります。

指定ルータおよびバックアップ指定ルータの選択には，ルータのネットワークへのインタフェースに定義する priority(コンフィグレーションコマンド interface(ospf area モード) の priority サブコマンド) を使用します。指定ルータが存在しない場合，バックアップ指定ルータを指定ルータに選択します。指定ルータもバックアップ指定ルータも存在しない場合は最も priority の高いルータを指定ルータに選択します。指定ルータは存在するが，バックアップ指定ルータが存在しない場合，指定ルータを除いて最も priority の高いルータをバックアップ指定ルータに選択します。両ルータとも存在する場合，新しくより priority の高いルータが現れても，選択は変更しません。

あるルータのあるインタフェースの priority を 0 と定義すると，このルータはインタフェースが接続しているエリアについて，指定ルータにもバックアップ指定ルータにも選択されません。

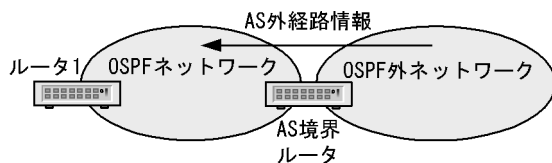
ブロードキャスト型ネットワーク上に複数のルータがあり，このネットワークをトラフィックの転送に使用する場合は，どれかのルータのネットワークに接続しているインタフェースの priority を 1 以上にする必要があります。

(a) 指定ルータについての注意事項

接続しているルータ数の多いネットワークでは，指定ルータの負荷は高くなります。このため，このようなネットワークに複数接続しているルータが存在する場合，このルータが複数のネットワークの指定ルータにならないように，priority を設定することをお勧めします。

12.5.5 AS 外経路と AS 境界ルータ

OSPF では，OSPF を使用しているルータが AS 外の経路情報を認識している場合，この経路を OSPF を使用してそのほかすべての OSPF を使用しているルータに通知できます。OSPF を使用し，AS 外経路を OSPF 内に導入するルータを **AS 境界ルータ**と呼びます。本装置を AS 境界ルータとして使用するためには，エキスポート・フィルタのコンフィグレーション (コンフィグレーションコマンド export の配布先プロトコルに ospfase を指定) が必要となります。AS 外経路情報の導入の概念を次の図に示します。

図 12-33　AS 外経路情報の導入の概念

(1) AS 外経路の広告

OSPF へ AS 外経路を導入するとき，導入元の AS 境界ルータは，宛先までのメトリック，AS 外経路メトリックタイプ，フォワーディングアドレスとタグを付加して広告します。

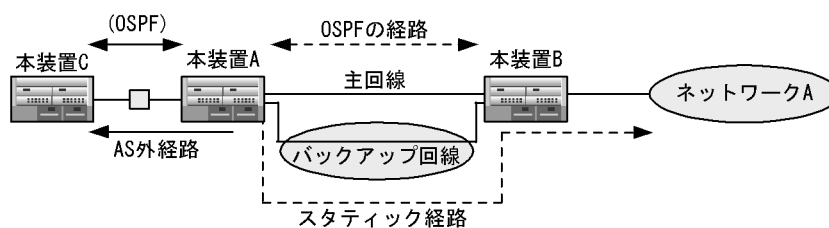
- メトリック
  宛先までのメトリックとして，固定の値を指定します (コンフィグレーションコマンド defaults(ospf モード) の cost サブコマンド，コンフィグレーションコマンド route-filter または export の metric パラメータ)。また，RIP のようにメトリックの情報を含んだ経路情報を OSPF へ取り込む場合には，メトリック引き継ぎ指定 (コンフィグレーションコマンド defaults(ospf モード) の inherit-metric サブコマンド) によって，メトリックを引き継ぐことができます。
- AS 外経路メトリックタイプ
  OSPF へ導入する AS 外経路には，Type 1 と Type 2 の 2 種類があります。Type 1 と Type 2 の経路では，経路の優先順位，およびメトリックを経路の選択に使用するときの計算方法が異なります。
- フォワーディングアドレス (転送先)
  転送先として使用する OSPF で到達可能なアドレスです。OSPF で到達可能でない場合，またはネクストホップのインタフェースがポイント - ポイント型である場合は 0.0.0.0 を設定します。なお，コンフィグレーションコマンド defaults(ospf モード) の suppress-forwarding-address サブコマンドを指定した場合，本装置が生成する AS 外経路のフォワーディングアドレスは，常に 0.0.0.0 を設定します。
  NSSA のエリアボーダルータでは，NSSA 内で学習した AS 外経路を別エリアに広告する際，フォワーディングアドレスを引き継ぎます。ただし，AS 外経路の導入元である NSSA について，コンフィグレーションコマンド area(ospf モード) の suppress-forwarding-address-type7to5 サブコマンドを指定

した場合，本装置が広告する AS 外経路のフォワーディングアドレスは，常に 0.0.0.0 を設定します。

- タグ
  付加情報としてタグを広告できます。

(2) AS 外経路の導入例

バックアップ回線を使用した構成での AS 外経路の導入例を次の図に示します。

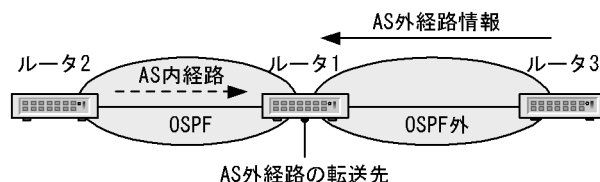
図 12-34　バックアップ回線を使用した構成での AS 外経路の導入例

OSPF では，隣接するルータを検出するために，定期的にパケットを交換します。このため，バックアップ回線を OSPF のトポロジの一部として使用した場合，この回線でパケットを継続して交換するため，バックアップ回線も常に運用状態になります。バックアップ回線上での通信が必要ではない場合にバックアップ回線を休止状態とするには，次のように設定します。

本装置 A では主回線で OSPF を動作させ，バックアップ回線にネットワーク A へのスタティック経路を定義します。デフォルトでは，OSPF の AS 内経路のプリファレンス値はスタティック経路のプリファレンス値と比べ小さい (優先度が高い) ため，ネットワーク A への経路は OSPF で学習した AS 内経路が選択されます。主回線障害時，本装置 A では該当する AS 内経路が削除されスタティック経路を再選択しますが，本装置 C ではネットワーク A への経路情報が存在しなくなります。本装置 A でのネットワーク A へのスタティック経路情報を AS 外経路として本装置 C に広告するためには本装置 A でエキスポート定義を設定する必要があります。こうすることによって，バックアップ回線上で Hello パケットを交換しないで主回線障害時にも OSPF にネットワーク A への有用な経路情報を導入できます。

(3) AS 外経路宛てのパケットの転送先

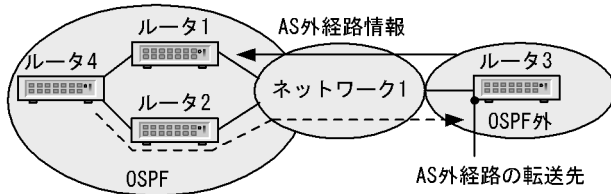
(a) AS 境界ルータを目標とする場合

AS 境界ルータを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1 がルータ 3 より学習した経路を AS 外経路として導入するに当たって，転送先をルータ 1 とします。ルータ 1 までの経路には，AS 内経路選択で選択した経路を使用します。

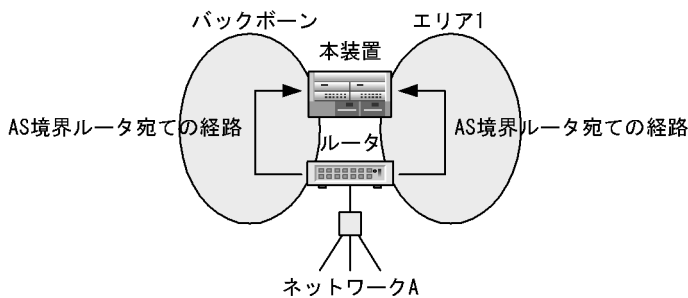
図 12-35　システム構成例 (AS 境界ルータを目標とする場合)

(b) フォワーディングアドレスを目標とする場合

フォワーディングアドレスを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1(AS 境界ルータ) がルータ 3 より学習した経路を AS 外経路として導入する当たって転送先をルータ 3 の

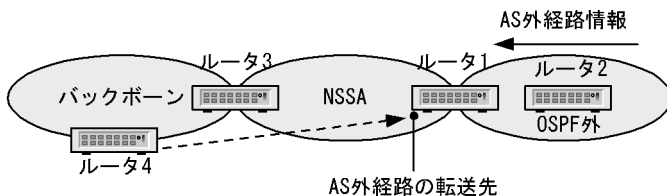
ネットワーク 1 へのインタフェースのアドレス (フォワーディングアドレス) とします。ルータ 4 から ネットワーク 1 に転送する場合，ルータ 2 経由の経路の方がコストが少ない場合は，導入した外部経路宛てのパケットの転送にルータ 2 経由の経路を選択します。

図 12-36　システム構成例 (フォワーディングアドレスを目標とする場合)

(c)　AS 外経路についての注意事項

AS 境界ルータ宛ての経路を次の図に示します。この例では，本装置 A はネットワーク A 宛ての AS 外経路をバックボーンエリアとエリア 1 の両方から学習します。このような場合，最初に学習した (すでに学習した経路の学習元) エリアを経由するパスを選択します。

図 12-37　AS 境界ルータ宛ての経路

(4)　NSSA 内の AS 外経路のパケット転送先

経路情報を AS 外経路として導入する場合，必ず AS 外経路に転送先アドレスを記します。経路情報の導入元がブロードキャスト型の OSPF インタフェースである場合，転送先は導入元アドレスになります。そのほかの条件では，転送先は NSSA 内の任意のインタフェースアドレスになります。任意のインタフェースを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1 がルータ 2 より学習した経路を AS 外経路として導入するときに，転送先を NSSA 内の任意のインタフェースにします。ルータ 4 は AS 外経路に記された転送先への経路を，エリア間経路選択によって選択します。

図 12-38　システム構成例 (任意のインタフェースを目標とする場合)

(a)　NSSA についての注意事項

AS 外経路の転送先アドレスは，NSSA 内の OSPF が動作しているインタフェースの中から選択します。インタフェースがダウンした場合は変更します。転送先アドレスの変更後，新しい AS 外経路を広告する

までの間，経路がいったん削除されることがあります。転送先を固定するため，経路情報の導入元であるブロードキャスト型インタフェースを，OSPF インタフェースとして定義することをお勧めします。

12.5.6　認証

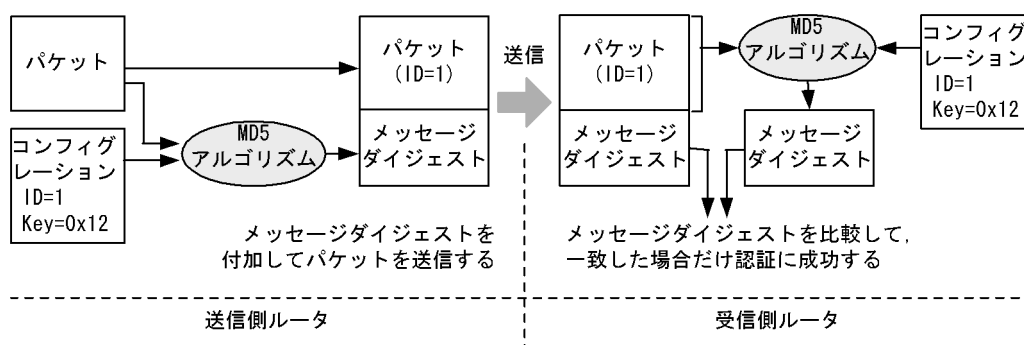
OSPF では，ルータ間の経路情報の交換時に情報を送信したルータが同じ管理下にあることを検証するために，認証を使用できます。認証を使用することで，OSPF の経路情報を送信されることによる経路制御上の攻撃から，認証管理下にあるルータを保護できます。認証方式には，平文パスワードによる認証と MD5 による認証があります。

（1） 平文パスワード認証

平文パスワード認証では，第一認証鍵と第二認証鍵を定義することができます。経路情報の送信時は，認証鍵をそのままパスワードとして埋め込んで送信します。このとき，パスワードとして使用する認証鍵は第一認証鍵です。経路情報の受信時は，両方の鍵を使用します。経路情報中のパスワードと，定義してある認証鍵のどれかが一致した場合，認証に成功したとみなします。認証に失敗した情報は破棄します。

（2） MD5 認証

MD5 認証では，経路情報に基づく MD5 アルゴリズムによるメッセージダイジェストを比較することで，情報を認証します。MD5 認証のデータフローを次の図に示します。

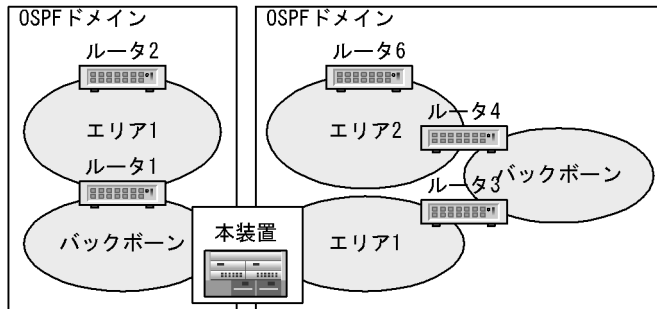
図 12-39　MD5 認証のデータフロー

経路情報の送信時には，認証鍵，認証鍵の ID，および経路情報自体から，MD5 ハッシュアルゴリズムを使用してメッセージダイジェストを生成し，これを経路情報とともに送信します。送信時の認証鍵には，現在の時刻を送信有効期間に含んでいる認証鍵を使用します。現在の時刻を送信有効期間に含む認証鍵が複数ある場合，送信有効開始時刻が現在時刻に最も近い認証鍵を使用します。有効な認証鍵が一つも存在しない場合は，最後に有効だった認証鍵を継続して使用します。

経路情報の受信時には，現在の時刻を受信有効期間に含んでいる認証鍵のうち，経路情報中に含まれる認証鍵の ID 番号と同じ ID 番号の認証鍵をすべて試します。この認証鍵を使用し，送信時と同様の手順を経てメッセージダイジェストを生成し，どれかの認証鍵から生成したメッセージダイジェストが経路情報とともに受信したメッセージダイジェストと一致した場合，認証に成功したとみなします。受信した情報について有効な鍵をすべて使用しても認証に成功しなかった場合は，この情報の認証に失敗したものとみなします。認証に失敗した情報は破棄します。

認証鍵の定義には，認証鍵自体と，認証鍵の ID 番号を必ず指定します。さらに，認証鍵に時刻の制限が必要な場合は受信有効期間および送信有効期間をそれぞれ開始時刻と終了時刻で定義できます。

12.5.7 OSPF マルチバックボーン機能

本装置では，1 台のルータ上で AS を複数の OSPF ネットワークに分割し，OSPF ネットワークごとに別個に経路の交換，計算，生成を行うことができます。この機能を **OSPF マルチバックボーン**と呼びます。OSPF マルチバックボーン機能の構成例を次の図に示します。以降，独立した各 OSPF ネットワークのことを，**OSPF ドメイン**と呼びます。OSPF ドメインは，最大四つ定義できます。

図 12-40　OSPF マルチバックボーン機能の構成例

1 台のルータが接続している複数の OSPF ドメインは，それぞれ独立した OSPF ネットワークとして動作します。このため，経路再配布についてのコンフィグレーションの定義がない場合には，一方の OSPF ドメイン上の経路が他方の OSPF ドメインへ配布されることはありません。すなわち，各ドメインは互いに異なるプロトコルとして動作します。経路再配布については「12.6　経路フィルタリング (RIP/OSPF)」を参照してください。

(1) OSPF ドメイン間の経路優先

複数の OSPF ドメインに同じ宛先への経路がある場合，OSPF の AS 内経路ならドメイン番号の小さいドメインの経路が優先されます。同じ宛先の AS 内経路と AS 外経路がある場合，通常は AS 内経路が優先されます。AS 外経路では，基本的にドメイン番号の小さい OSPF ドメインの経路が優先されます。ただし，AS 外経路では，コンフィグレーションコマンド import の preference パラメータまたはコンフィグレーションコマンド defaults(ospf モード) の preference サブコマンドによってプレファレンス (優先度) 値を指定できます。この場合，指定したプレファレンス値の小さい方の経路を優先します。OSPF ドメイン間の経路優先の例を次の図に示します。

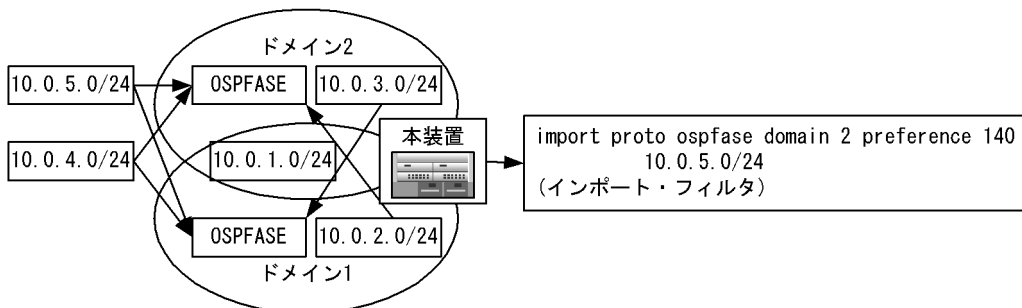
図 12-41　OSPF ドメイン間の経路優先の例

この図の構成例では，次の表に示すような OSPF ドメイン間の経路優先が行われます。

表 12-17　OSPF ドメイン間の経路優先

宛先	ドメイン 1	ドメイン 2	優先する経路を含むドメイン	備考
10.0.1.0/24	10 (OSPF)	10 (OSPF)	ドメイン 1	ドメイン番号
10.0.2.0/24	10 (OSPF)	150 (OSPFASE)	ドメイン 1	プリファレンス値
10.0.3.0/24	150 (OSPFASE)	10 (OSPF)	ドメイン 2	プリファレンス値
10.0.4.0/24	150 (OSPFASE)	150 (OSPFASE)	ドメイン 1	ドメイン番号
10.0.5.0/24	150 (OSPFASE)	140 (OSPFASE)	ドメイン 2	プリファレンス値（インポート・フィルタ）

(2) マルチバックボーン機能使用時の注意事項

(a) マルチバックボーン使用についての注意

ネットワークを複数の OSPF ドメインに分割して運用した場合，ルーティンググループの抑止やコストに基づいた経路選択などの OSPF の特長が，OSPF ドメイン間の経路の選択や配布によって失われます。新規ネットワーク構築時など，ネットワークを複数の OSPF ドメインに分割して運用する必要がない場合には，単一の OSPF ネットワークとして構築することをお勧めします。

(b) 複数ドメイン使用時のインタフェース定義についての注意

インタフェースを同時に複数の OSPF ドメインに定義しないでください。本装置に接続している各インタフェースは，それぞれ一つのドメインの一つのエリアだけに所属できます。複数のドメインで OSPF インタフェースとして定義した場合，対象のインタフェースは，どの OSPF ドメインでも OSPF インタフェースとして動作しなくなります。

(c) 装置アドレス使用についての注意

装置アドレスを複数の OSPF ドメインに広告する必要がある場合には，OSPF AS 外経路として広告してください。装置アドレスを OSPF AS 外経路として広告するには，「12.6.2　エキスポート・フィルタ (RIP/OSPF)」を参照してください。

12.5.8 経路選択の優先順位

本装置は，各プロトコルで学習した同一宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同一宛先への経路情報が各プロトコルでの生成によって複数存在する場合，それぞれの経路情報のプリファレンス値が比較され優先度の最も高い経路情報が有効となります。OSPF 内における経路選択の優先順位を次の表に示します。

表 12-18　経路選択の優先順位

優先順位	選択項目	詳細
高	経路情報の種類	OSPF の AS 内経路は，AS 外経路より優先します。
↑	学習元ドメイン	• 複数ドメインに経路が存在する場合，プリファレンス値が最小である経路を選択します。プリファレンス値が等しい場合，OSPF ドメイン番号が最小の経路を選択します。
	経路の宛先タイプ	• AS 内経路：エリア内経路は，エリア間経路より優先します。 • AS 外経路：エリア内の AS 境界ルータが広告している経路が，別エリアの AS 境界ルータが広告している経路よりも優先します。
	AS 外経路タイプ	Type1 の AS 外経路は，Type 2 の AS 外経路より優先します。

優先順位	選択項目	詳細
	AS 外経路で経由するエリア	エリアボーダであるルータでは，宛先の AS 境界ルータが複数のエリアに接続している場合，AS 境界ルータまでのコスト値が最も小さいエリアを選択します。コスト値が等しい場合，エリア ID の最も大きいエリアを選択します。
	コスト	• AS 内経路：宛先までのコスト値が最も小さい経路を優先します。 • Type1 の AS 外経路：AS 外経路情報のメトリック値と AS 境界ルータまでのコスト値の合計が最も小さい経路を優先します。 • Type2 の AS 外経路：AS 外経路情報のメトリック値が最も小さい経路を選択する。メトリック値が等しい場合，AS 境界ルータまでのコスト値が最も小さい経路を選択します。
↓ 低	ネクストホップアドレス	ネクストホップアドレスが最も小さいアドレスを選択します。

注 1

コンフィグレーションコマンド ospf の multipath サブコマンドを定義することによって，AS 内経路について，学習元ドメインと宛先タイプとコストが等しい経路を複数選択できます。AS 外経路についても同様に，学習元ドメインと AS 外経路タイプとコストが等しい経路を複数選択できます。

注 2

選択項目の優先順位は変更できません。

12.5.9 グレースフル・リスタート

(1) 概要

グレースフル・リスタートは，装置の BCU が系切替したり，運用コマンドなどによりルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機能です。グレースフル・リスタート機能一般については，「12.8 グレースフル・リスタートの概要」を参照してください。

OSPF では，グレースフル・リスタートによって OSPF の再起動を行う装置のことをリスタートルータといいます。リスタートルータにあるグレースフル・リスタートをする機能をリスタート機能といいます。また，グレースフル・リスタートを補助する隣接装置をヘルパールータといいます。ヘルパールータにあるグレースフル・リスタートを補助する機能をヘルパー機能といいます。

SB-7800S では，リスタート機能とヘルパー機能をサポートしています。

SB-5400S では，ヘルパー機能だけをサポートしています。

OSPF のコンフィグレーションでは，ドメインごとにリスタート機能とヘルパー機能の動作可否を指定できます。

以下に，OSPF でグレースフル・リスタート機能を使用するときの構成上の条件を示します。以下の条件を満たさない場合，グレースフル・リスタートに失敗したり，グレースフル・リスタートが終了するまで通信できない経路ができたりすることがあります。

- グレースフル・リスタートするルータに，リスタート機能を設定してください。本装置でリスタート機能を設定する場合，コンフィグレーションコマンド options で graceful-restart パラメータを設定し，コンフィグレーション ospf コマンドの graceful-restart サブコマンドで mode restart または mode both を設定してください。
- グレースフル・リスタートするルータの隣接ルータすべてに，ヘルパー機能を設定してください。本装置でヘルパー機能を設定する場合，コンフィグレーションコマンド ospf の graceful-restart サブコマンドで mode helper または mode both を設定してください。

(2) リスタート機能【SB-7800S】

(a) リスタート機能の動作契機

以下に，本装置で OSPF のリスタート機能が動作する契機を示します。

- BCU が系切替したとき。
- ルーティングプログラムが再起動したとき。

(b) グレースフル・リスタートの手順

次の図および表に OSPF のグレースフル・リスタート手順を示します。

図 12-42　OSPF グレースフル・リスタート手順

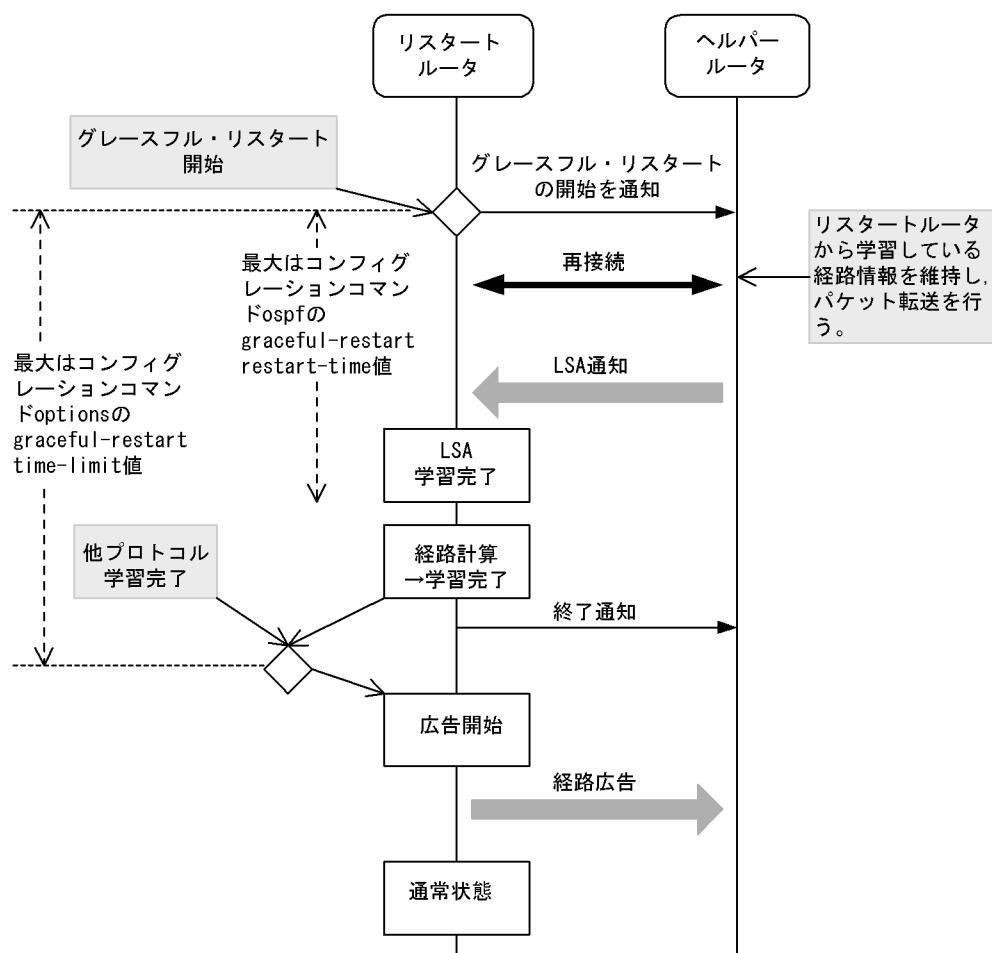



表 12-19　OSPF グレースフル・リスタート手順

項番	項目	契機	処理内容
1	グレースフル・リスタートの開始	BCU が系切替したとき。	グレースフル・リスタートを開始します。通常の接続手順と同様に，各インタフェースで OSPF 情報のパケット交換を行います。
		ルーティングプログラムが再起動したとき。	

項番	項目	契機	処理内容
2	経路計算	ドメイン内の全 OSPF インタフェースについて再接続完了し，隣接ルータからすべての LSA を学習したとき。	ドメインごとに経路計算を行い，ルーティングテーブルを更新します。 複数のドメインが存在する場合，経路計算は接続の終わったドメインから随時行います。経路計算が全ドメインで終了したとき，OSPF の経路学習が完了します。
		1 インタフェースでもグレースフル・リスタートに失敗したとき。	その時点での同一ドメイン内の各インタフェースの接続状態に基づいて，経路計算を行います。
3	広告開始	OSPF の経路学習が完了し，かつほかのルーティングプロトコルの経路学習が完了したとき。	AS 外経路の広告を開始します。広告完了後，通常の OSPF 動作に戻ります。
		OSPF のグレースフル・リスタートに失敗したとき。	

(c) グレースフル・リスタートが失敗するケース

以下に OSPF のグレースフル・リスタートが失敗するケースを示します。

- グレースフル・リスタートの開始をヘルパールータへ通知してからコンフィグレーションコマンド ospf の graceful-restart restart-time の時間が経過しても LSA 学習を完了できなかった場合。
- 再接続を行っているインタフェースがダウンした場合。
- OSPF ドメイン上で LSA が変更された場合。
- OSPF ドメイン上の別のルータがグレースフル・リスタートした場合。
- グレースフル・リスタートを開始してから経路保持時間 (コンフィグレーションコマンド options の graceful-restart time-limit の時間) が経過しても全プロトコルの経路学習が完了しなかった場合。
- コンフィグレーションコマンド ospf の graceful-restart mode を変更し，リスタートルータ機能を削除した場合。
- コンフィグレーションコマンド options を変更し，グレースフル・リスタート機能を削除した場合。

(d) 注意事項

1. リスタートルータとして，グレースフル・リスタートを開始しても，一部のヘルパールータがヘルパー動作を開始しない場合や，途中で止めた場合，同一ドメイン内の全インタフェースでグレースフル・リスタートを止めます。
2. OSPF のリスタート時間 (コンフィグレーションコマンド ospf の graceful-restart restart-time の時間) を，系切替所要時間 + LSA 学習時間を超えるように設定してください。これは，OSPF が LSA を学習するためには，系切替が完了して IP インタフェースの Up/Down が確認できるようになっている必要があるためです。グレースフル・リスタート開始後，リスタート時間が経過した時点で LSA の学習が終わってない場合，OSPF のグレースフル・リスタートに失敗します。
   系切替所要時間については，「表 12-30　系切替所要時間の目安値」を参照してください。
3. 本装置の系切替時ルーティングエントリ保持時間を，OSPF のリスタート時間よりも長く設定してください。OSPF のリスタート時間よりもルーティングエントリ保持時間のほうが短い場合，経路学習前に系切替前ルーティングエントリが削除されることがあります。
4. BGP4 のルーティングピアがグレースフル・リスタートを使用している場合，ルーティングピアのリスタート時間を OSPF のリスタート時間よりも長く設定してください。
   ルーティングピアのリスタート時間のほうが短い場合，OSPF が経路学習を完了する前にルーティングピアを接続することができず，ルーティングピアのグレースフル・リスタートに失敗することがあります。

（3） ヘルパー機能

本装置は，ヘルパールータとして動作している場合，グレースフル・リスタートを行っている間，リスタートルータを経由する経路を維持します。

（a） ヘルパー機能の動作条件

ヘルパー機能が動作する条件を以下に示します。

- 既に同一ドメイン内で別のリスタートルータのヘルパーとなっていないこと。同一ドメイン内で，複数のルータのグレースフル・リスタートに対して同時にヘルパールータとして動作できません。ただし，リスタートルータが 1 台しかない場合，そのリスタートルータと接続しているインタフェースすべてでヘルパールータとして動作を行います。
- 自ルータがリスタートルータとして，グレースフル・リスタートを実行していないこと。**【SB-7800S】**
- リスタートルータに送信した OSPF の Update パケットに対する Ack 待ちの状態でないこと。

（b） ヘルパー機能が失敗するケース

ヘルパールータとしての動作は，隣接が確立するまで，または，リスタートルータから終了の通知を受信するまで継続します。

しかし，以下のイベントが発生した場合，リスタートルータが維持している経路と不整合が発生する可能性があるため，ヘルパー機能を中断し，経路を再計算します。

- 隣接ルータから新しい LSA(定期更新を除く) を学習し，リスタートルータへ広告した場合。
- OSPF インタフェースがダウンした場合。
- リスタートルータ以外のルータとの隣接関係の切断または確立によって LSA を更新した場合。
- OSPF の同一ドメイン内で，複数のルータが同時に再起動した場合。
- コンフィグレーションコマンド ospf の graceful-restart mode を変更し，ヘルパー機能を削除した場合。

（c） 注意事項

1. 本装置の OSPF 隣接ルータで OSPF リスタート機能を使用する場合，本装置に OSPF ヘルパー機能を設定してください。

12.5.10 スタブルータ

（1） 概要

隣接ルータとの接続が完了していなかったり，安定していなかったりすると，ネットワーク全体のルーティングが不安定になることがあります。ルータの起動時・再起動時やネットワークにルータを追加するときに，このような状況がおこることがあります。OSPF ではこのような状況下，周辺の装置でルーティングにできるだけ使用されないように，経路情報を通知することができます。OSPF では，このような通知を行っているルータを，スタブルータと呼びます。この機能によって，装置の状態が不安定であっても，ネットワークのルーティングが不安定になることを防ぐことができます。

（2） スタブルータ動作

スタブルータは，接続する OSPF インタフェースのコスト値を最大値（65535）にして広告します。このため，スタブルータを経由する OSPF 経路は優先されなくなります。

ただし，隣接ルータの存在しないインタフェース（スタブネットワーク）の経路については，コンフィグレーションで指定したコスト値を広告します。スタブネットワークや AS 外経路はスタブルータの経路が優先されることがあります。

周辺装置では，コスト比較により，スタブルータを経由しない代替経路を優先します。また，スタブルー

タ自身の装置アドレスを使用して，telnet，SNMP による管理や BGP4 による経路交換ができます。

OSPF のコンフィグレーションでは，ドメインごとにスタブルータ機能を動作させるかどうかを指定できます。さらに，動作条件として，スタブルータとして常時動作させるか，または起動後に動作させるかを選択できます。

(3) 常時動作する場合

常時，コストを最大値にします。スタブルータのコンフィグレーションを削除するまで，動作し続けます。

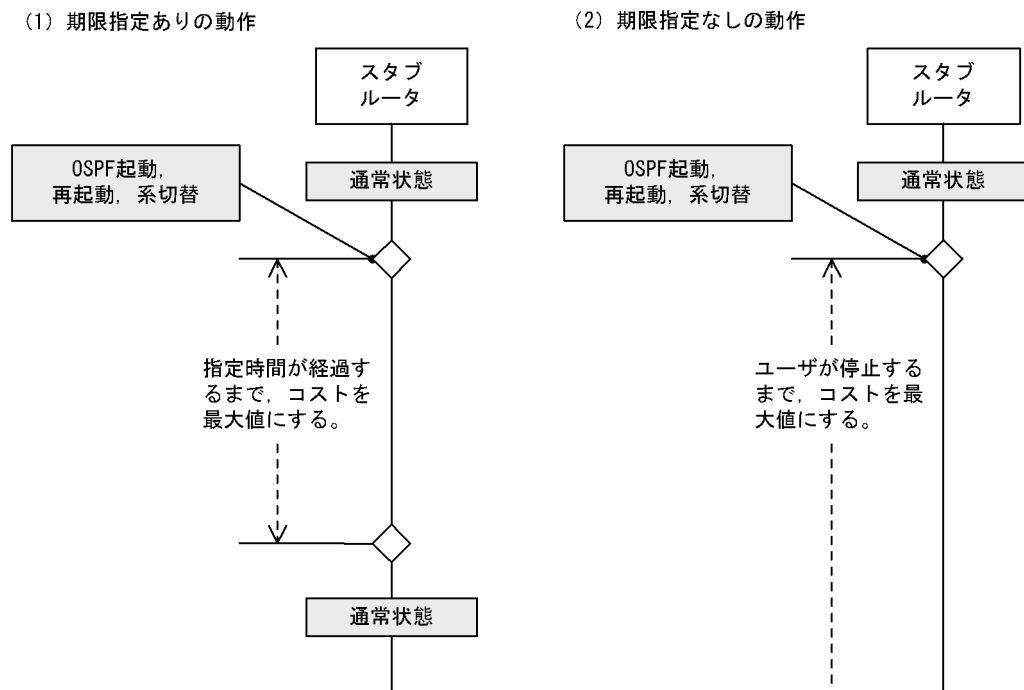
(4) 起動後にスタブルータとして動作する場合

次に示す契機でコストを最大値にします。コンフィグレーションで指定した期限が経過するまで，継続します。

- BCU の系切替後（グレースフル・リスタート成功時を除く）
- ルーティングプログラムの再起動後（グレースフル・リスタート成功時を除く）
- グレースフル・リスタートが発生し，本装置がリスタートルータとしての経路学習に失敗した後
- 装置起動

コンフィグレーションを変更し，起動後にスタブルータとして動作することを指定した場合，次回の起動・再起動・系切替から適用されます。

動作中に運用コマンド clear ip ospf stub-router を実行するか，コンフィグレーションを削除することで停止できます。スタブルータの動作を次の図に示します。

図 12-43　スタブルータの動作

(5) 注意事項

1. グレースフル・リスタートのヘルパールータとして動作しているとき，スタブルータのコンフィグレーションを変更しないでください。定義を変更すると，スタブルータが動作を開始したり，終了したりして，ヘルパー動作に失敗することがあります。
2. スタブルータとして常時動作する定義になっているとき，起動後に動作するように変更すると，すぐに

スタブルータを終了します。

3. 仮想リンクの通過エリアでのコストが 65535 よりも大きい場合，仮想ネーバはその仮想リンクを到達不能とみなします。このため，スタブルータを通過する仮想リンクは，使用できません。
4. 古い OSPF 規格の RFC1247 の仕様では，最大メトリックの経路情報は，SPF 計算に使用されません。このため，新しい OSPF 規格に対応していない装置では，スタブルータを経由する経路は登録されません。

12.5.11 高速経路切替機能

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報 (第 1 優先経路と呼ぶ) と，第 1 優先経路の次に優先される経路 (第 2 優先経路と呼ぶ) をあらかじめルーティングテーブルに登録しておき，インタフェースダウンによって第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディング・テーブルに登録することで，通信停止時間の短縮を図る機能です。

OSPF 単独で第 1 優先経路と第 2 優先経路の両方をルーティングテーブルに登録することはできませんが，スタティック経路など OSPF 以外のプロトコルで生成した同一宛先の経路を組み合わせることによって，この機能を適用することが可能です (「表 13-7　高速経路切替を適用する経路の組み合わせ」を参照してください)。

高速経路切替機能の詳細については「13.2.5　高速経路切替機能」を参照してください。

12.5.12 OSPF 使用時の注意事項

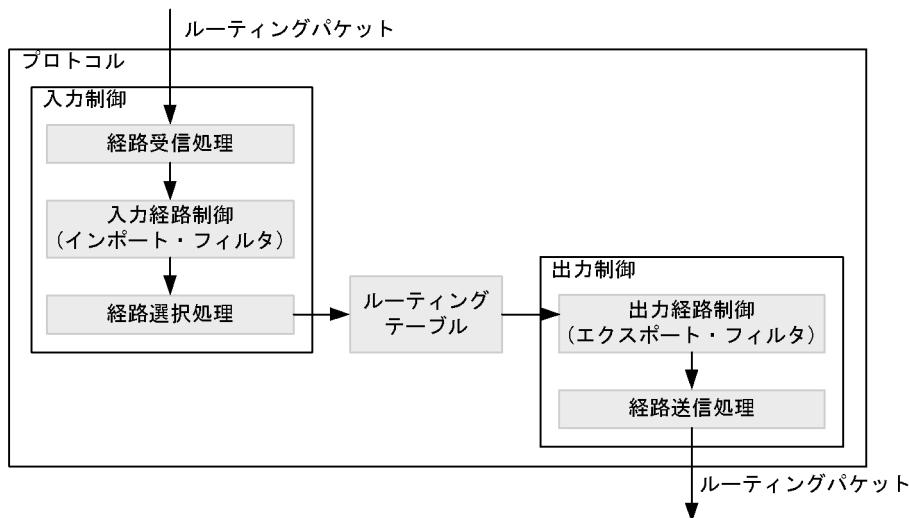
OSPF を使用したネットワークを構成する場合には，次の制限事項に留意してください。

- OSPF の制限事項
  本装置は，RFC2328(OSPF バージョン 2) に準拠していますが，ソフトウェアの機能制限によって，Point-to-MultiPoint インタフェースはサポートしていません。
- NSSA の制限事項
  本装置は，RFC1587(The OSPF NSSA Option) に準拠していますが，ソフトウェアの機能制限によって，次に示す機能はサポートしていません。
  - Type-7 Address Ranges
  - Type-7 Translator Election

  このため，NSSA から学習した AS 外経路を常に NSSA でないエリアに広告します。
- Opaque LSA の制限事項
  本装置は，Type9 の Opaque LSA の学習，広告を行いますが，OSPF のグレースフル・リスタートに使用する grace-LSA 以外の機能は，サポートしていません。
  なお，Type10，Type11 の Opaque LSA の学習，広告はサポートしていません。

12.6　経路フィルタリング (RIP/OSPF)

経路フィルタリングには，入力経路を制御する**インポート・フィルタ**と出力経路を制御する**エキスポート・フィルタ**があります。インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。エキスポート・フィルタは同一ルーティングプロトコル，またはルータ上で同時に動作している異なるプロトコルで学習した経路を広告するかどうかを制御します。フィルタリングの概念を次の図に示します。

図 12-44　フィルタリングの概念

12.6.1　インポート・フィルタ (RIP/OSPF)

インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。インポート・フィルタを指定していない場合は，すべての経路情報を取り込みます。

（1） プリファレンス値

取り込む経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，そのプロトコルのデフォルトのプリファレンス値になります。

同一宛先アドレスの経路情報が複数存在する場合，プリファレンス値によって優先度の高い経路情報が有効となります。プリファレンス値の詳細は，「12.3.3　スタティックルーティングとダイナミックルーティング (RIP/OSPF) の同時動作　(1) プリファレンス値」を参照ください。

（2） フィルタリング条件

取り込む経路情報はフィルタリング条件で指定できます。指定できるインポート・フィルタのフィルタリング条件を次の表に示します。

表 12-20　インポート・フィルタのフィルタリング条件

プロトコル	フィルタリング条件
RIP	• 受信インタフェース • 送信元ゲートウェイ • 経路情報の宛先ネットワーク
OSPFASE ※	• OSPF ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク

注※　OSPF の AS 外経路

12.6.2　エキスポート・フィルタ (RIP/OSPF)

エキスポート機能はルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。学習元プロトコルで学習した経路情報を，配布先プロトコルを使用してほかのシステム (ルータ) に広告します。

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件 (送出先) と学習元プロトコルのフィルタリング条件 (送出経路情報) によって特定の宛先に特定の経路情報を送出できます。

(1)　フィルタリング条件

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件 (送出先) と学習元プロトコルのフィルタリング条件 (送出経路情報) によって，特定の宛先に特定の経路情報を送出できます。また，配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値となります。

指定できるフィルタリング条件を配布先プロトコルと学習元プロトコルに分け「表 12-21　配布先プロトコルのフィルタリング条件」と「表 12-22　学習元プロトコルのフィルタリング条件」に示します。なお，配布先プロトコルが，BGP4 の場合は，「13.4.2　エキスポート・フィルタ (BGP4)」を参照してください。

表 12-21　配布先プロトコルのフィルタリング条件

配布先プロトコル	フィルタリング条件 (送出先)	付加情報
RIP	• 送信先インタフェース	• メトリック値
OSPFASE	• OSPF ドメイン番号 ただし，学習元が同じ OSPF ドメインの OSPF, OSPFASE の場合は制御できません。	• メトリック値 • AS 外経路タイプ • タグ値

表 12-22　学習元プロトコルのフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIP	• 受信インタフェース • 送信元ゲートウェイ • 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIP で学習された経路情報
OSPF	• OSPF ドメイン番号 • 経路情報の宛先ネットワーク	OSPF で学習された経路情報
OSPFASE	• OSPF ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPF の AS 外経路情報

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
DIRECT	• インタフェース • 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 送出元インタフェース • 経路情報の宛先ネットワーク	スタティックの経路情報
DEFAULT【**OP-BGP**】	• 経路情報の宛先ネットワーク	BGP4 の DEFAULT 経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

(2) 再配布する経路情報のメトリック値

フィルタリング条件には再配布する経路情報のメトリック値，またはメトリック値に加算する値を指定できます。RIP で再配布する経路情報のメトリック値を「表 12-23　再配布する経路情報のメトリック値 (RIP)」に，OSPF で再配布する経路情報のメトリック値を「表 12-24　再配布する経路情報のメトリック値 (OSPFASE)【OP-OSPF(SB-5400S)】」に示します。また，フィルタリング条件でオフセット指定 (+ 指定) した場合に，RIP で再配布する経路情報のメトリック値を「表 12-25　オフセット指定した場合に再配布する経路情報のメトリック値 (RIP)」に，OSPF で再配布する経路情報のメトリック値を「表 12-26　オフセット指定した場合に再配布する経路情報のメトリック値 (OSPFASE)【OP-OSPF(SB-5400S)】」に示します。

表 12-23　再配布する経路情報のメトリック値 (RIP)

metric 指定	学習元プロトコル	メトリック値
あり	RIP	経路情報のメトリック値を引き継ぐ。
	その他	エキスポート・フィルタで指定したメトリック値を使用します。
なし	RIP	経路情報のメトリック値を引き継ぎます。
	直結経路	直結経路 (ブロードキャスト型回線) の場合，1 で広告します。直結経路 (ポイント - ポイント型回線の自装置側インタフェース) の場合，1 で広告します。直結経路 (ポイント - ポイント型回線の相手装置側インタフェース) の場合，2 で広告します。
	集約経路	集約経路の場合，1 で広告します。
	OSPF，OSPFASE，BGP4，IS-IS	コンフィグレーションコマンド rip の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値または MED 属性値を引き継ぎます。ただし，値が 1~15 以外の場合は，RIP として広告しません。そのほかの場合，デフォルト・メトリック値を使用します。
	スタティック経路，デフォルト経路	デフォルト・メトリック値を使用します。

表 12-24　再配布する経路情報のメトリック値 (OSPFASE)【**OP-OSPF(SB-5400S)**】

metric 指定	学習元プロトコル	メトリック値
あり	全プロトコル共通	エキスポート・フィルタで指定したメトリック値を使用します。
なし	OSPF	コンフィグレーションコマンド defaults(ospf モード) の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値を引き継ぎ，経路の種類が type1 になります。これ以外でコンフィグレーションコマンド ospf の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。

metric 指定	学習元プロトコル	メトリック値
	OSPFASE(Type1)	コンフィグレーションコマンド rip の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値と経路の種類 (type 1) およびタグ値を引き継ぎます。これ以外でコンフィグレーションコマンド ospf の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。
	OSPFASE(Type 2)	コンフィグレーションコマンド rip の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値に 1 を加えた値と経路の種類 (type 2) およびタグ値を引き継ぎます。これ以外でコンフィグレーションコマンド ospf の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。
	RIP，直結経路，集約経路，BGP4，スタティック経路，デフォルト経路，IS-IS	コンフィグレーションコマンド rip の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値を引き継ぎます。経路情報にメトリック値または MED 属性値がない場合は，0 を使用します。また，値が 16777215(10 進数) 以上の場合は，OSPFASE として広告しません。経路の種類はデフォルト (ospf コマンドで指定のない場合は type2) になります。上記以外でコンフィグレーションコマンド ospf の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。

注　学習元プロトコルの OSPF，OSPFASE は配布先と異なるドメインに所属する OSPF，OSPFASE を示します。同一ドメインへの経路情報は再配布しません。

表 12-25　オフセット指定した場合に再配布する経路情報のメトリック値 (RIP)

学習元プロトコル	メトリック値
RIP，直結経路，集約経路，スタティック経路，デフォルト経路，	「表 12-23　再配布する経路情報のメトリック値 (RIP)」に示すメトリック値に，オフセット値を加算した値を使用します。
BGP4，OSPF，OSPFASE，IS-IS	「表 12-23　再配布する経路情報のメトリック値 (RIP)」に示すメトリック値に，オフセット値を加算した値を使用します。ただし，コンフィグレーションコマンド rip の inherit-metric サブコマンド指定によって，引き継いだメトリック値，または MED 属性値が 0 の場合は，0 を基準にオフセット値を加算した値を使用します。

注　オフセット値の加算結果が 16 以上になった場合，経路情報は再配布しません。

表 12-26　オフセット指定した場合に再配布する経路情報のメトリック値 (OSPFASE)【OP-OSPF(SB-5400S)】

学習元プロトコル	メトリック値
OSPF，OSPFASE	ドメイン間で経路情報を再配布する場合は，「表 12-24　再配布する経路情報のメトリック値 (OSPFASE)【OP-OSPF(SB-5400S)】」に示すメトリック値に，オフセット値を加算した値を使用します。(注 : 同一ドメインへの経路情報の再配布は行わないため，オフセット値の加算も行いません)
RIP，BGP4，直結経路，集約経路，スタティック経路，デフォルト経路，IS-IS	「表 12-24　再配布する経路情報のメトリック値 (OSPFASE)【OP-OSPF(SB-5400S)】」に示すメトリック値に，オフセット値を加算した値を使用します。

注　オフセット値の加算結果が 16777215 以上になった場合，経路情報は再配布しません。

12.7 経路集約 (RIP/OSPF)

経路集約は一つまたは複数の経路情報から該当する経路情報を包含するようなネットワークマスクのより短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含するような一つの経路情報を生成し，隣接ルータなどに集約経路を通知することでネットワーク上の経路情報の数を少なくする手法です。例えば，172.16.178.0/24 の経路情報や 172.16.179.0/24 の経路情報を学習した場合に 172.16.0.0/16 の集約された経路情報を生成するなどです。

経路集約の指定はコンフィグレーションコマンド aggregate(経路集約) で明示的に指定する必要があります。集約元の経路情報はフィルタリング条件によって特定できます。集約元経路情報のフィルタリング条件を次の表に示します。

表 12-27　集約元経路情報のフィルタリング条件

集約元プロトコル	フィルタリング条件 (集約元経路情報)	備考
RIP	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIP で学習された経路情報
OSPF	• 経路情報の宛先ネットワーク	OSPF で学習された経路情報
OSPFASE	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPF の AS 外経路情報
DIRECT	• 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 経路情報の宛先ネットワーク	スタティックの経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

また，集約元経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定することができます。プリファレンス値を指定していない場合は，集約経路のデフォルトのプリファレンス値 (130) が使用されます。なお，集約元の経路情報が学習されていない場合には集約経路情報は生成されません。

(1) 集約元経路の広告抑止

経路集約後，集約経路については広告するが集約元となった経路については広告対象外にできます。例えば，集約元経路以外の RIP 経路は広告したいが集約元の RIP 経路を広告しないなどです。

集約元経路の広告抑止は集約経路単位または全集約経路に対して指定できます。集約経路単位に指定する場合は，コンフィグレーションコマンド aggregate の summary-only サブコマンドで指定します。全集約経路を対象とする場合はコンフィグレーションコマンド options の summary-only パラメータで指定します。

集約元経路の広告抑止の適用例を次の図に示します。

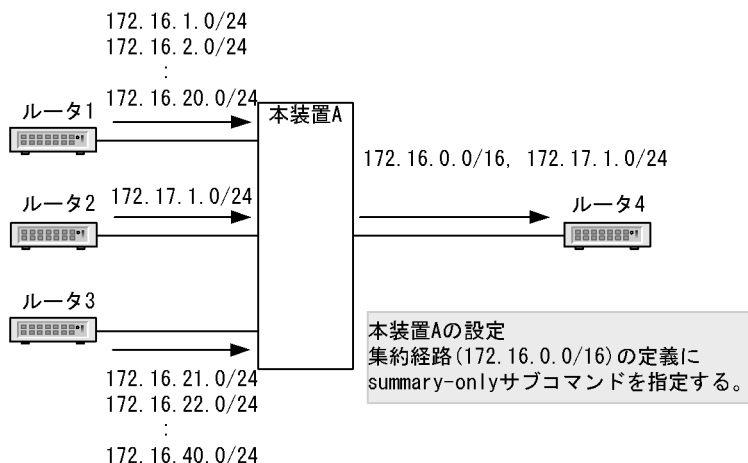
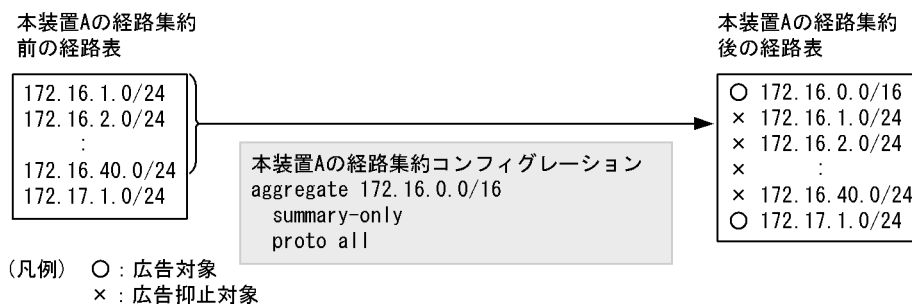
図 12-45　集約元経路の広告抑止の適用例

本装置 A は，ルータ 1 より 172.16.1.0/24，172.16.2.0/24，…，172.16.20.0/24 を受信し，ルータ 2 より 172.17.1.0/24 を受信し，ルータ 3 より 172.16.21.0/24，172.16.22.0/24，…，172.16.40.0/24 を学習します。本装置 A では，集約経路 172.16.0.0/16 と学習経路 172.17.1.0/24 をルータ 4 へ広告するようにエキスポート・フィルタを定義します。このとき，summary-only サブコマンドを指定して学習経路から集約経路 172.16.0.0/16 を生成するように定義した場合，エキスポート・フィルタに集約元経路の広告を抑止する設定が不要となります。経路集約コンフィグレーション例と経路集約前後の経路を次の図に示します。

図 12-46　経路集約コンフィグレーション例と経路集約前後の経路

(2) 集約経路の転送方法

集約経路はリジェクト経路です。より優先する経路がないパケットは廃棄されます。

集約経路がリジェクト経路になっているのは，ルーティングループを防ぐためです。集約経路を広告すると，その集約経路宛てのパケットが本装置へ転送されてきます。ここで本装置が集約元経路の無いパケットをデフォルト経路などの次善の経路に従って転送すると，デフォルト経路転送先装置と本装置の間でルーティングループが発生することがあります。これを防ぐため，集約経路はリジェクト経路になっています。

ただし，noinstall サブコマンドを指定した集約経路はパケットを廃棄しません。デフォルト経路など次善の経路がある場合は，その経路に従ってパケットを転送します。noinstall サブコマンドは，広告用に集約経路を設定したいが，その集約経路でパケットを廃棄するよりも次善の経路に従って転送した方がよい場合に使用します。

12.8 グレースフル・リスタートの概要

12.8.1 SB-7800S でのグレースフル・リスタート【SB-7800S】

（1） 概要

グレースフル・リスタートは，装置の BCU が系切替したり，運用コマンドなどによりユニキャストルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機能です。

（2） グレースフル・リスタートを使用しない場合の問題

本装置では，装置の BCU が系切替したり，運用コマンドなどによってユニキャストルーティングプログラムが再起動したりしても，本装置がパケット転送を中断することはありません。これは，本装置では PSU にもルーティングテーブルがあるため，ルーティングプログラムを切り替えても以前のルーティングプログラムの経路を保留して動作し続けているためです。

しかし，ルーティングプロトコルを使用している場合，隣接ルータが本装置へパケットを転送しなくなるため，ネットワーク全体では通信が一時的に停止することがあります。これは以下の理由によります。

- 新たに動作を始めたルーティングプログラムが隣接ルータと通信を開始すると，隣接ルータは新たな接続要求を受け取ります。これによって，隣接ルータでは以前の接続が切断したものと認識し，該当装置を経由する経路を削除します。
- 本装置が一部の経路を広告しません。これは，新しく動作を開始したルーティングプログラムが経路広告を開始した時点では，まだ経路情報の学習が完了していないためです。隣接ルータでは，本装置が広告しなかった経路を削除します。

（3） グレースフル・リスタートによる解決方法

グレースフル・リスタートは，上記問題を解決することによってルーティングプログラム切替時の通信停止時間を短縮する機能です。以下に具体的な解決方法を示します。

- 隣接ルータに，グレースフル・リスタートを補助する機能を用意します。グレースフル・リスタートによる接続要求を受け取ったときに，以前の接続を切断して再接続するのではなく，以前の接続を継続しているものと認識する機能を追加します。これによって，ルーティングプログラム切替時にも隣接ルータとの接続が切断しなくなるため，隣接ルータも経路を保持したまま動作します。
- 経路学習・経路広告の処理順序を固定します。グレースフル・リスタートするに当たり，まず隣接ルータから経路情報を学習し，経路学習が完了してから経路広告を開始します。これによって，一部経路しか広告しないことで隣接ルータから経路が消えることがなくなります。

なお，グレースフル・リスタートを実施するルータのことをリスタートルータと呼びます。

次の図と表に，本装置のグレースフル・リスタート動作手順を示します。

図 12-47　グレースフル・リスタート手順

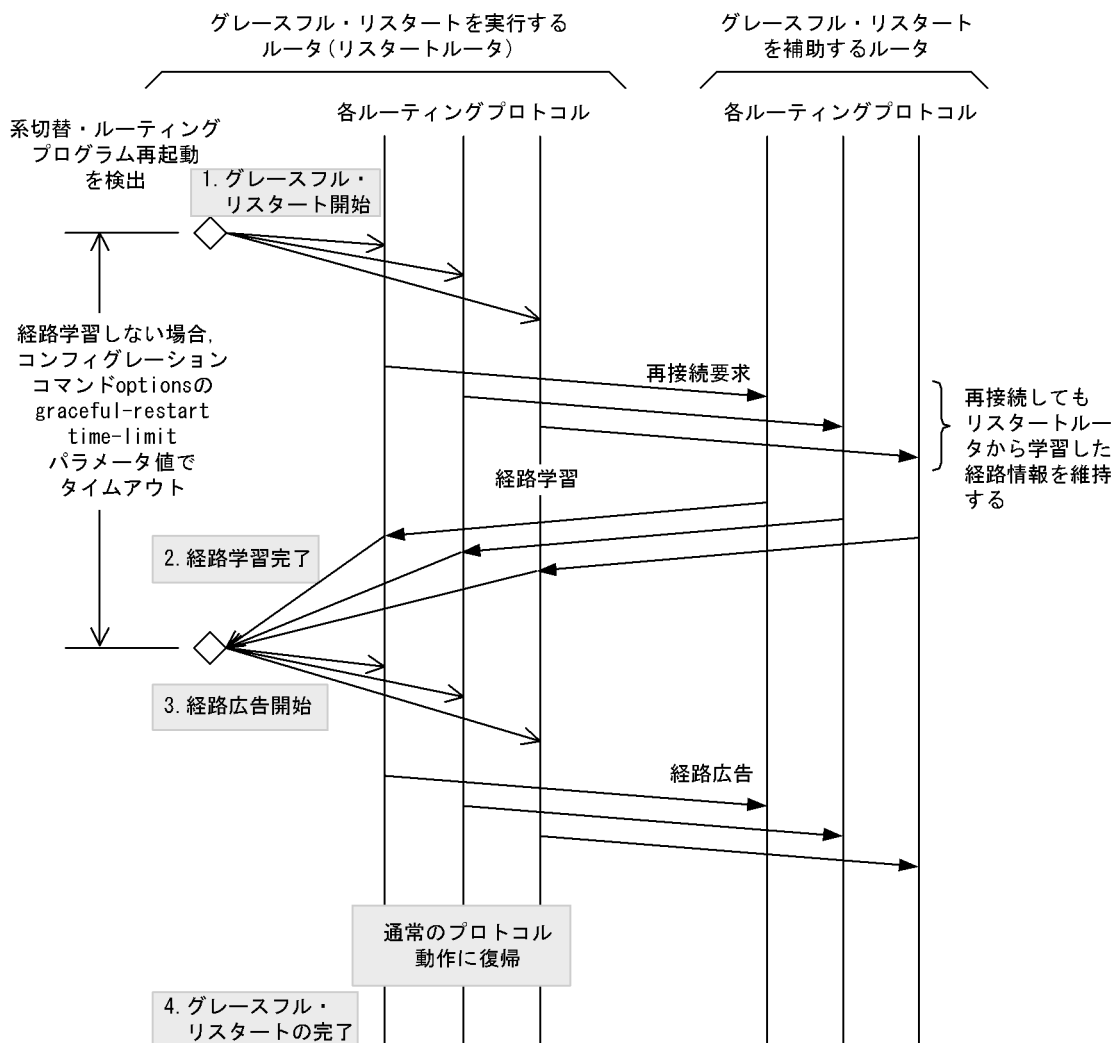



表 12-28　グレースフル・リスタート手順

項番	動作
1	系切替またはルーティングプログラムの再起動を検出すると，各プロトコルがグレースフル・リスタートを開始します。 各プロトコルは，グレースフル・リスタートによる再接続を行い，経路を学習します。
2	グレースフル・リスタート対象の各プロトコルが経路学習を完了します。
3	経路学習の完了後，グレースフル・リスタート対象の各プロトコルは経路広告を開始します。
4	各プロトコルは，経路広告を完了したら通常のプロトコル動作に復帰します。 全プロトコルが経路を広告し終わった時点で，装置全体のグレースフル・リスタートが完了します。

（4） グレースフル・リスタートのサポート範囲

グレースフル・リスタート機能のサポート範囲を次の表に示します。

表 12-29　グレースフル・リスタート機能のサポート範囲

項目		サポート
対象イベント	装置再起動	×

<table>
<tr><th colspan="3">項目</th><th>サポート</th></tr>
<tr><td rowspan="3"></td><td colspan="2">BCU 再起動</td><td>×</td></tr>
<tr><td colspan="2">BCU 系切替</td><td>○※1※2</td></tr>
<tr><td colspan="2">ユニキャストルーティングプログラム再起動</td><td>○※1</td></tr>
<tr><td rowspan="6">対象インタフェース</td><td rowspan="4">イーサネット</td><td>Line</td><td>○</td></tr>
<tr><td>Tag-VLAN 連携</td><td>○</td></tr>
<tr><td>リンクアグリゲーション</td><td>○※3※4</td></tr>
<tr><td>VLAN</td><td>○※5</td></tr>
<tr><td colspan="2">POS</td><td>○※6</td></tr>
<tr><td colspan="2">トンネル</td><td>×</td></tr>
<tr><td rowspan="2">対象フォワーディング・パケット</td><td colspan="2">IPv4 ユニキャスト</td><td>○※7※8</td></tr>
<tr><td colspan="2">IPv6 ユニキャスト</td><td>○※7※8</td></tr>
<tr><td rowspan="5">対象ルーティングプロトコル</td><td colspan="2">OSPF</td><td>○</td></tr>
<tr><td colspan="2">OSPFv3</td><td>○</td></tr>
<tr><td colspan="2">IS-IS</td><td>○</td></tr>
<tr><td colspan="2">BGP4</td><td>○</td></tr>
<tr><td colspan="2">BGP4+</td><td>○</td></tr>
</table>

（凡例） ○：取り扱う　×：取り扱わない

注※ 1

グレースフル・リスタート中に再度イベントが発生した場合には，グレースフル・リスタートしません。

注※ 2

本装置の系切替条件については，「解説書 Vol.2　4. 冗長構成」を参照してください。

注※ 3

LACP を使用するリンクアグリゲーションを除きます。本装置で LACP によるリンクアグリゲーション機能とグレースフル・リスタートを同時に使用すると，系切替時のグレースフル・リスタートに失敗します。これは，系切替時に LACP が障害を検出し，リンクアグリゲーションを通信不可状態にするためです。

注※ 4

系切替時にリンクアグリゲーションの MAC アドレスが変らないようにするため，コンフィグレーションコマンド local-mac-address の定義が必要です。

注※ 5

スパニングツリーを使用する VLAN を除きます。本装置でスパニングツリー機能を使用している場合，系切替時にグレースフル・リスタートを使用しても通信停止時間が発生します。これは，本装置が系切替すると，スパニングツリーが一時的に不安定な状態になり，通信ができなくなるためです。

注※ 6

PPP のリンク品質監視を使用する場合を除きます。本装置で PPP のリンク品質監視機能とグレースフル・リスタートを同時使用すると系切替時のグレースフル・リスタートに失敗します。これは，系切替時に回線品質低下を検出し，回線を切断するためです。

注※ 7

ソフトウェアによるフォワーディング・パケットを除きます。

・装置内でフラグメント化が必要なパケット

・オプション付きパケット

注※ 8

グレースフル・リスタート以外のサービス機能の中断により中継不可となるケースを除きます。例えば，以下の

ケースがあります。
・DHCP のサービス中断
・ARP/NDP の応答中断

(5) 設定可能なコンフィグレーションオプション

本装置では，装置全体でのグレースフル・リスタートの使用可否，グレースフル・リスタート時の経路保留時間，各プロトコルのグレースフル・リスタート機能，および各プロトコルのグレースフル・リスタート補助機能を設定することができます。また，グレースフル・リスタート機能とグレースフル・リスタート補助機能を同時に設定することもできます。

(6) 関連するマニュアル記載事項

グレースフル・リスタートの動作方式はプロトコルによって異なるため，動作条件も異なります。使用前に，各プロトコルのグレースフル・リスタート動作条件をご確認ください。各プロトコルの個別機能については，以下を参照してください。

- OSPF　　:「12.5.9　グレースフル・リスタート」
- BGP4　　:「13.3.11　グレースフル・リスタート」
- IS-IS　　:「14.2.8　グレースフル・リスタート」
- OSPFv3　:「17.5.8　グレースフル・リスタート」
- BGP4+　:「18.3.11　グレースフル・リスタート」

また，本装置の系切替時にグレースフル・リスタートを使用する場合，本装置の系切替条件をご確認ください。系切替による経路引き継ぎ条件および動作手順については，「解説書 Vol.2　4. 冗長構成」を参照してください。

(7) 使用上の注意事項

1. 障害による系切替の場合，系切替が完了しグレースフル・リスタートによる再学習を始めるよりも前に，隣接装置が切断を検出することがあります。各プロトコルの切断検出時間を，系切替所要時間よりも長くなるようにしてください。以下に，デフォルト値で運用したときのプロトコル別の切断検出までの最短時間の目安値を示します。
   OSPF，OSPFv3：　25 秒
   BGP4，BGP4+ ：100 秒
   IS-IS　　　　：　5 秒
   系切替所要時間はインタフェース数に依存します。「表 12-30　系切替所要時間の目安値」の時間を目安としてください。
   運用コマンドによる系切替でグレースフル・リスタートを使用する場合，各プロトコルのリスタート時間を，系切替所要時間よりも長くなるように指定してください。

表 12-30　系切替所要時間の目安値

インタフェース数※	系切替所要時間 (秒)
250	22
1,000	45
2,000	85
4,000	160

注※　同一インタフェースそれぞれに IPv4 アドレスと IPv6 アドレスを定義した場合。

2. OSPF・OSPFv3・IS-IS のリスタート時間を，系切替所要時間と経路学習時間の和よりも長くしてください。これは，経路情報を同期するためには，系切替を完了して IP インタフェースの Up/Down 状

態が確認できるようになる必要があるためです。
系切替所要時間については，「表 12-30　系切替所要時間の目安値」を参照してください。

3. BGP4・BGP4+ のリスタート時間を，系切替所要時間とコネクション確立にかかる時間の和よりも長くしてください。これは，BGP4・BGP4+ ピアのコネクションを確立するためには，系切替を完了して IP インタフェースの状態を確認できるようになる必要があるためです。
さらに，BGP4，BGP4+ でルーティングピアを使用している場合には，BGP4・BGP4+ のリスタート時間を，OSPF・OSPFv3・IS-IS のリスタート時間とピアのコネクション確立にかかる時間の和よりも長くしてください。これは，BGP4・BGP4+ ルーティングピアのコネクションを確立するためには，ルーティングピアに使用する IGP がグレースフル・リスタートにより経路を学習しておく必要があるためです。
4. グレースフル・リスタート時の経路保留時間 (コンフィグレーションコマンド options の graceful-restart time-limit パラメータ指定値) を，各プロトコルのリスタート時間よりも長く設定してください。OSPF，OSPFv3，ISIS では，リスタート時間が，経路計算の実施を待つ時間の上限となります。したがって，経路保留時間がリスタート時間以下の場合，経路計算によってフォワーディング・テーブルを更新するより先に，保留経路 (更新されていないフォワーディング・テーブル) の削除が実行されるので，通信が停止します。また，BGP4 と BGP4+ では，リスタート時間が BGP コネクションの再確立を待つ時間の上限となるので，再確立が最も遅い場合は，リスタート時間後に BGP4 ピアからの経路学習を開始します。経路学習およびフォワーディング・テーブルを更新する時間のため，BGP4 と BGP4+ のリスタート時間は経路保留時間より 60 秒程度短い値を設定してください。なお，目安の設定値は経路数および隣接する BGP4 ピア数に依存します。
5. グレースフル・リスタート中はコンフィグレーションを変更しないでください。グレースフル・リスタート中にコンフィグレーションを変更するとグレースフル・リスタートに失敗することがあります。
6. グレースフル・リスタート中は，グレースフル・リスタートの補助機能が動作しません。
7. グレースフル・リスタート中に隣接ルータで障害が発生した場合，グレースフル・リスタートに失敗することがあります。
8. グレースフル・リスタート手順が成功しても，隣接装置で，本装置から学習した経路情報を保持できなかった場合，通信が停止することがあります。

12.8.2　SB-5400S でのグレースフル・リスタート【SB-5400S】

本装置では，系切替時やルーティングプログラムの再起動時のグレースフル・リスタート機能はサポートしませんが，隣接ルータがグレースフル・リスタートする場合に，その動作を補助するグレースフル・リスタート補助機能をサポートします。本機能は，グレースフル・リスタートを実行するルータ (リスタートルータ) からグレースフル・リスタートによる再接続要求を受けた場合にリスタートルータから学習した経路情報を維持し，パケットフォワーディングを継続します。

本装置でグレースフル・リスタート補助機能に対応しているプロトコルは，OSPF，BGP4，IS-IS，OSPFv3，BGP4+ です。グレースフル・リスタート補助機能のプロトコル個別機能については，以下を参照してください。

- OSPF　　:「12.5.9　グレースフル・リスタート」
- BGP4　　:「13.3.11　グレースフル・リスタート」
- IS-IS　　:「14.2.8　グレースフル・リスタート」
- OSPFv3　:「17.5.8　グレースフル・リスタート」
- BGP4+　:「18.3.11　グレースフル・リスタート」

12.9 複数プロトコル同時動作時の注意事項

RIP または OSPF を複数同時動作させた場合の注意事項について説明します。

12.9.1 OSPF または RIP-2 と RIP-1 の同時動作

OSPF や RIP-2 は IP アドレスの ClassA，B，C を意識しないで可変長サブネットマスクを扱うルーティングプロトコルであるのに対して，RIP-1 は ClassA，B，C を前提としているため可変長サブネットマスクは扱えません。したがって，両者を同ネットワークで混在して使用する場合には次に示す注意が必要です。この項では OSPF と RIP-1 の関係を例に説明しますが，RIP-2 と RIP-1 の関係も同様です。

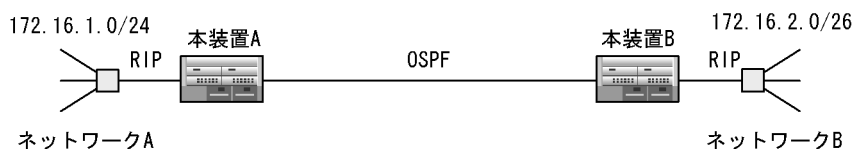
（1） OSPF で学習したサブネット経路を RIP-1 で広告しない場合

サブネッティングされたネットワークへの経路は次に示すどちらかの条件に当てはまる場合，該当する経路を RIP-1 で広告しないので注意してください。

1. RIP を使用しているインタフェースのネットワークアドレスと異なるサブネットマスク長を持つサブネットへの経路。
2. RIP を使用しているインタフェースのネットワークアドレスと異なるネットワークアドレスのサブネットへの経路。

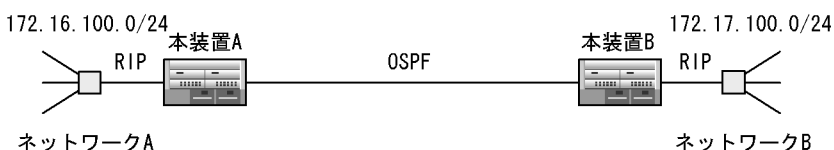
（a） 異なるサブネットマスク長のサブネット間の接続

次の図の本装置 A の場合，ネットワーク B への経路を自分のルーティングテーブルに登録します，このとき，ネットワーク B が前に示した 1 の条件に当てはまるため，ネットワーク A にネットワーク B の経路を広告しません。

図 12-48　異なるサブネットマスク長のサブネット間の接続

「図 12-51　サブネット間の接続の例」の本装置 A の場合，ネットワーク A とネットワーク B は同一ネットワーク内の同一サブネット長のサブネットのために経路を広告します。

（b） 異なるネットワークアドレスのサブネット間の接続

次の図の本装置 A の場合，ネットワーク B への経路を自分のルーティングテーブルに登録しますが，ネットワーク B が前に示した 2 の条件に当てはまるため，ネットワーク A にネットワーク B の経路を広告しません。

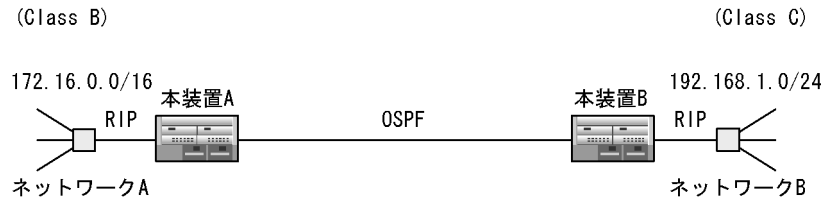
図 12-49　異なるネットワークアドレスのサブネット間の接続

「図 12-51　サブネット間の接続の例」の本装置 A の場合，ネットワーク A とネットワーク B は同一ネットワーク内の同一サブネット長のサブネットのために経路を広告します。

（2） OSPF による RIP のネットワーク間接続

RIP が動作しているネットワーク間を OSPF で接続する場合は，次に示すどれかの構成で接続してください。

（a） サブネットを使用しない。

次の図の場合，ネットワーク A，ネットワーク B への経路情報は，それぞれネットワーク B，ネットワーク A に広告されます。

図 12-50　サブネットを使用しない例

（b） 同一ネットワークで同一サブネット長のサブネット間の接続に使用する。

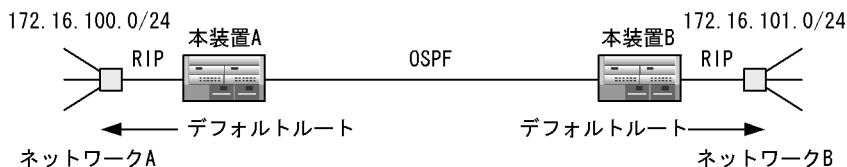
次の図の場合，ネットワーク A，ネットワーク B への経路情報は，それぞれネットワーク B，ネットワーク A に広告されます。

図 12-51　サブネット間の接続の例

（c） デフォルトルートを広告する。

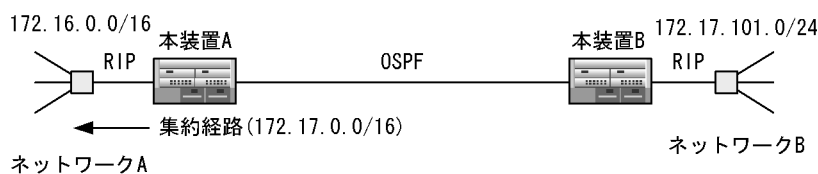
本装置 A および本装置 B に宛先がデフォルトルートのスタティック経路を定義し，RIP が動作しているネットワークに広告します。

次の図の場合，デフォルトルートの広告によって宛先アドレスが自ネットワークに一致しないパケットはデフォルトルートによって本装置 A および本装置 B に到達し，OSPF 経路経由で相手のネットワークに配送されます。

図 12-52　デフォルトルートの広告の例

（d） 集約経路を広告する。

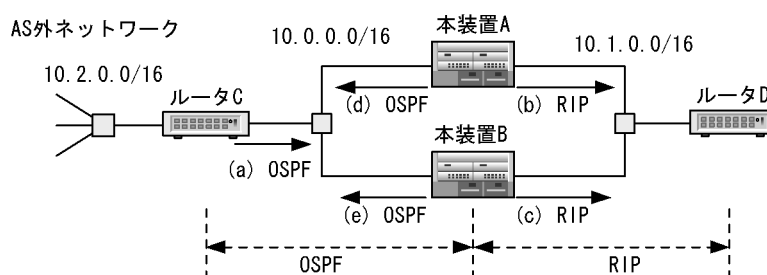
本装置 A に学習元が OSPF/OSPFASE(OSPF の AS 外経路) であるネットワーク B 宛ての経路をナチュラルマスクの経路に集約し，RIP が動作しているネットワークに広告するように指定します。

次の図の場合，集約経路の広告によってネットワーク B 宛てのパケットは本装置 A に到達し，OSPF/OSPFASE 経路経由で相手のネットワークに配送されます。

図 12-53　集約経路の広告の例

12.9.2　複数のプロトコルで同じ宛先の経路を学習する場合の注意事項

複数のプロトコルで同じ宛先の経路を学習すると，ネットワーク構成によってはルーティングループが発生することがあります。そのようなネットワーク構成では，経路のフィルタリングによってルーティングループが発生しないように注意してください。

次の図のネットワーク構成例では，10.0.0.0 のネットワークは OSPF を使用し，10.1.0.0 のネットワークでは RIP を使用しています。

図 12-54　ネットワーク構成例

ネットワーク 10.2.0.0 宛ての経路は次の 3 種類が生成されます。

1. ルータ C が広告する AS 外経路 (図の (a))
2. OSPF から RIP にエキスポートした経路 (図の (b)，(c))
3. RIP から OSPF にエキスポートした経路 (図の (d)，(e))

この例では本装置 B が (d) を選択し本装置 A が (c) を選択した場合，または本装置 A が (e) を選択し本装置 B が (b) を選択した場合にルーティングループ (ネクストホップがお互いのルータを向いている) が発生します。このようなケースでは本装置 A や本装置 B が OSPF から RIP に広告した 10.2.0.0 宛ての経路を RIP から OSPF の AS 外経路として学習しないようにフィルタリング (エキスポート・フィルタ) を設定する必要があります。

13 BGP4【OP-BGP】

この章では IPv4 のルーティングプロトコルの BGP4 について説明します。

13.1　BGP4 概説

BGP4(Border Gateway Protocol 4) は，プロバイダ間の多大な経路情報のやり取りが必要なインターネット接続に適用されるルーティングプロトコルで，階層型のネットワークの概念に基づいて作成されています。BGP4 はインターネットのバックボーン上で，プロバイダ間でルーティングテーブルを交換するときに使用されます。また，イントラネットを二つ以上の ISP に接続する場合に使用されます。

AS 内のルータ間の経路情報の交換には RIP や OSPF のような IGP(Interior Gateway Protocol) を使用します。BGP4 は，AS 間のルーティングプロトコルであり，EGP(Exterior Gateway Protocol) の一つです。BGP4 はインターネット上で使用されているすべての経路情報を扱えます。

BGP4 の機能を次の表に示します。

表 13-1　BGP4(IPv4) の機能

機能	BGP4
EBGP，IBGP ピアリング，経路配信	○
経路フィルタ，BGP 属性変更	○
コミュニティ	○
ルート・リフレクション	○
コンフィデレーション	○
サポート機能のネゴシエーション	○
ルート・リフレッシュ	○
マルチパス	○
ポリシーグループ※1	○
ルート・フラップ・ダンピング	○
BGP4 MIB	○
TCP MD5 認証	○
グレースフル・リスタート	○※2

（凡例）　○：取り扱う

注※ 1
外部ピア同士，または内部ピア同士のグルーピング

注※ 2
SB-5400S ではレシーブルータの機能だけサポートします。

13.1.1　経路情報

本装置が取り扱う経路情報（ルーティングの対象にするアドレスの種類）を次の表に示します。

表 13-2　経路情報

経路情報の種類		説明
通常の経路	デフォルト経路	すべてのネットワーク宛ての経路。 （宛先アドレス：0.0.0.0，ネットワークマスク：0.0.0.0）

経路情報の種類		説明
	ナチュラルマスク経路	アドレスクラスに対応したネットワークマスクの経路。(ネットワークマスク:クラスA=8ビット,クラスB=16ビット,クラスC=24ビット)
	サブネット経路	特定のサブネット宛ての経路。 (ネットワークマスクがアドレスクラスに対応したネットワークマスクよりも長い経路)
	ホスト経路	特定のホスト宛ての経路。(ネットワークマスクが32ビットの経路)
	可変長サブネットマスク	本装置の経路制御は可変長サブネットマスク:VLSM(Variable Length Subnet Mask)を取り扱います。同一ネットワークアドレスで,長さの異なる複数のサブネットマスクを取り扱えます。
CIDR対応の経路	スーパーネット経路	アドレスクラスに対応したネットワークマスクより短いネットワークマスクの経路情報を取り扱います。例えば,クラスCのネットワークアドレス192.168.8.0/24,192.168.9.0/24,192.168.10.0/24,192.168.11.0/24の経路情報を一つのスーパーネット経路192.168.8.0/22に集約し取り扱えます。
	0サブネット経路	サブネット番号が0のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば,クラスBのネットワークアドレス172.16.0.0/24の経路情報を取り扱えます。
	-1サブネット経路	サブネット番号が-1(All'1')のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば,クラスBのネットワークアドレス172.16.255.0/24の経路情報を取り扱えます。
	包括的サブネット	複数の経路情報間でネットワークアドレスが包括関係にある経路を別の経路情報として取り扱います。例えば,クラスBのネットワークアドレス172.16.3.0/24と172.16.2.0/23は個々の経路情報として取り扱われます。

13.1.2 BGP4の適用範囲

BGP4の適用範囲を次の表に示します。

表13-3 BGP4の適用範囲

経路情報		BGP4
経路情報	デフォルト経路	○
	ナチュラルマスク経路	○
	サブネット経路	○
	ホスト経路	○
	可変長サブネットマスク	○
	CIDR対応	○
	マルチパス	○
経路選択		ASパス属性
ルーティングループの抑止		○
認証機能		○

(凡例) ○:取り扱う

13.1.3　ネットワーク設計の考え方

本装置を使用しネットワークを設計する上で注意事項がありますので，「12.2　ネットワーク設計の考え方」を参照してください。

13.2 経路制御 (BGP4)

13.2.1 スタティックルーティング

スタティックルーティングはコンフィグレーションで設定した経路情報（スタティック経路）に従ってパケットを中継する機能です。スタティックルーティングについては「12.3.1　スタティックルーティング」を参照してください。

13.2.2 ダイナミックルーティング (BGP4)

本装置では RIP バージョン 1，RIP バージョン 2，OSPF バージョン 2，BGP バージョン 4，IS-IS をサポートしています。RIP については「12.4　RIP」に，OSPF については「12.5　OSPF【OP-OSPF(SB-5400S)】」に，BGP4 については「13　BGP4【OP-BGP】」に，IS-IS については「14　IS-IS【OP-ISIS】」に示します。

13.2.3 スタティックルーティングとダイナミックルーティング (BGP4) の同時動作

(1) プリファレンス値

複数のルーティング種別が同時動作するとき，それぞれは独立した経路選択手順に従い，ある宛先アドレスへの経路情報から一つの最適の経路を選択します。その結果，ルータ内ではある宛先アドレスへの経路情報が複数存在することになります。このような場合，それぞれの経路情報のプリファレンス値が比較されて優先度の高い経路情報が有効になります。

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコル（例えば BGP4）ごとに生成する経路情報のデフォルトのプリファレンス（優先度）値をコンフィグレーションで設定できます。なお，プリファレンスは値の小さい方の優先度が高くなります。各プロトコルのプリファレンスのデフォルト値を次の表に示します。

表 13-4　プリファレンスのデフォルト値

経路	デフォルトプリファレンス値
直結経路	0(固定値）
OSPF の AS 内経路	10
IS-IS の内部経路	15
BGP4 のデフォルト経路	20
スタティック経路	60
RIP 経路	100
集約経路	130
OSPF の AS 外経路	150
IS-IS の外部経路	160
BGP4 経路	170

(2) エキスポート機能

本装置では，学習した経路情報を BGP4 で広告したい場合や，特定の経路情報の広告をフィルタリングしたい場合にはエキスポート機能によって実現できます。

エキスポート機能では，コンフィグレーションで学習元プロトコルと配布先プロトコル (BGP4) を指定することによって，特定ルーティングプロトコルで学習した経路を BGP4 で広告することができます。

(a) BGP4 で学習した経路の広告

BGP4 経路のエキスポート設定をしていない場合，同一ルーティングプロトコルで学習した経路情報であっても広告されません。ある AS から学習した BGP4 経路を他の AS に広告するためにはエキスポートの定義が必要です。

エキスポートの設定によって広告される経路情報は BGP4 で選択された最適の経路です。

(b) BGP4 以外で学習した経路の広告

複数のルーティングプロトコルが同時動作するとき，BGP4 以外のルーティングプロトコルで学習した経路情報はエキスポートの定義をすることで広告されます。

エキスポートの設定によって広告される経路情報はプリファレンス値によって選択された最も優先度の高い経路です。

(c) 同一宛先経路の広告

BGP4 で学習した経路情報と他のルーティングプロトコルで学習した経路情報が同一宛先である場合，エキスポートの設定により広告される経路情報が異なります。同一宛先経路の広告条件を次の表に示します。

表 13-5 同一宛先経路の広告条件

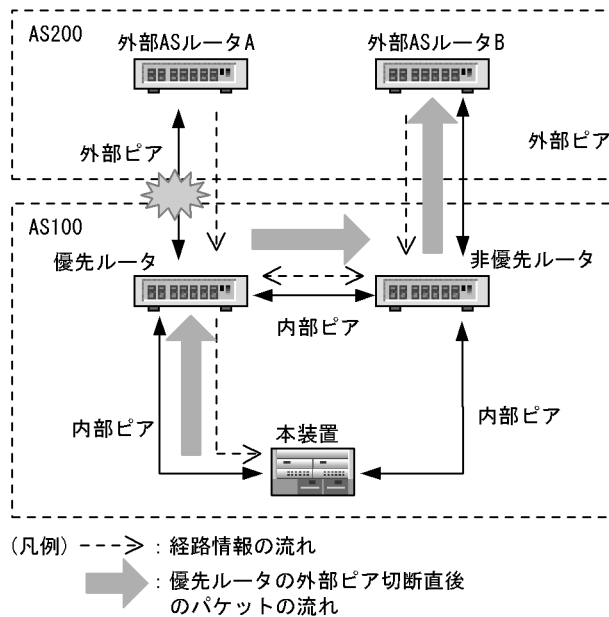
学習元プロトコルの エキスポート許可指定		広告条件
BGP4	BGP4 以外※	
未指定	未指定	広告しません。
	指定	• 指定した学習元プロトコルで学習した経路情報の内，プリファレンス値によって選択された最も優先度の高い経路情報を広告します。 • 学習した経路情報の優先度が低い場合はエキスポートを設定しても広告しません。
指定	未指定	• BGP4 で学習した経路情報のうち，最適の経路を広告します。 • BGP4 以外で学習した経路情報が BGP4 の経路情報より優先度の高い場合でも，BGP4 経路を広告します。
	指定	• 指定した学習元プロトコルで学習した経路情報のうち，プリファレンス値によって選択された最も優先度の高い経路情報を広告します。 • BGP4 以外で学習した経路情報の方が優先度が高い場合，その経路情報がエキスポート対象でなければ最適の BGP4 経路を広告します。

注※ RIP，OSPF，OSPFASE，DIRECT，STATIC，DEFAULT，AGGREGATE のどれかを示します。

13.2.4 経路削除保留機能

経路削除保留機能は，ルーティングプロトコルが無効にした経路を，ルーティングテーブルから一定時間削除しないようにすることで，新しく代替経路が生成されるまでの間，既存経路によってフォワーディングを維持する機能です。

経路削除保留機能の適用例を次の図に示します。

図 13-1 経路削除保留機能の適用例

上図で優先ルータと外部 AS ルータ A 間のピア切断によって，本装置の BGP4 経路は非優先ルータから再学習するまでの間，一時的に無効となりますが，経路削除保留機能を適用しているためルーティングテーブルからは経路情報が削除されず，下記の経路でパケットフォワーディングが維持されます。

[優先ルータ→非優先ルータ→外部 AS ルータ B]

13.2.5 高速経路切替機能

(1) 概要

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報（第 1 優先経路と呼ぶ）と，第 1 優先経路の次に優先される経路（第 2 優先経路と呼ぶ）をあらかじめルーティングテーブルに登録しておき，インタフェースダウンなどによって第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディングテーブルに登録することで，通信停止時間の短縮を図る機能です。

高速経路切替のサポート範囲を次の表に示します。

表 13-6 高速経路切替のサポート範囲

切替契機	切替内容
インタフェースダウン	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わない IGP 経路の変更による BGP 経路の NextHop 変更	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わないピア切断による BGP 経路の NextHop 変更	第 2 優先経路への切り替え
	マルチパス経路の縮退

高速経路切替を適用する経路の組み合わせを次の表に示します。

表 13-7 高速経路切替を適用する経路の組み合わせ

項目		第 1 優先経路※ 3 ※ 4								
		BGP4	OSPF	RIP	IS-IS	スタティック (gateway 指定) ※ 1	スタティック (remote-gateway 指定) ※ 1	スタティック (interface 指定) ※ 1 ※ 2	集約経路	直結経路
第 2 優先経路 ※ 3 ※ 4	BGP4	○	○	○	○	○	○	○	×	×
	OSPF	○	-	○	○	○	○	○	×	×
	RIP	○	○	○	○	○	○	○	×	×
	IS-IS	○	○	○	-	○	○	○	×	×
	スタティック (gateway 指定) ※ 1	○	○	○	○	○	○	○	×	×
	スタティック (remote-gateway 指定) ※ 1	○	○	○	○	○	○	○	×	×
	スタティック (interface 指定) ※ 1 ※ 2	○	○	○	○	○	○	○	×	×
	集約経路	×	×	×	×	×	×	×	-	×
	直結経路	×	×	×	×	×	×	×	×	-

(凡例) ○：適用する　×：適用しない　-：この組み合わせは発生しない

注※ 1
コンフィグレーションコマンド static の reject サブコマンドまたは noinstall サブコマンドを指定した場合は高速経路切替を適用しない。

注※ 2
Null インタフェース，local-address または broadcast 型インタフェースを指定した場合は高速経路切替を適用しない。

注※ 3
IPv4 over IPv6 トンネルを送出インタフェースとする経路については高速経路切替を適用しない。

注※ 4
第 1 優先経路または第 2 優先経路をルーティングテーブルに追加後，本経路に高速経路切替機能が適用されるまで，1 万経路当たり約 3 秒の時間を要します。
その間，経路切替契機が発生しても，高速経路切替が適用されない場合があります。

(2) BGP4 プロトコルによる適用例 (第 2 優先経路への切り替え)

次の図の様に，BGP4 プロトコルが複数のピアから学習した同一宛先の経路情報で高速経路切替を行うには，コンフィグレーションコマンド options の fast-reroute パラメータと，コンフィグレーションコマンド bgp の fast-reroute サブコマンドで gen-secondary-route パラメータを設定し，第 2 優先経路を生成する必要があります。この場合，「13.3.2　経路選択アルゴリズム」で示す優先順位が，最も高い経路が第 1 優先経路に，2 番目に高い経路が第 2 優先経路に選択されます。なお，第 1 優先経路と第 2 優先経路のプリファレンス値が同じ値でない場合には，第 2 優先経路は生成しません。

図 13-2 BGP4 プロトコルによる高速経路切替機能の適用例 (第 2 優先経路への切り替え)

(a) 経路切り替え前

(b) 経路切り替え後

この図で本装置 A は，ネットワーク B 宛の経路情報を学習した本装置 B および本装置 D とピアを形成し，ネットワーク B 宛の経路情報を本装置 B および本装置 D のそれぞれから学習しています。本装置 B から学習した経路情報は本装置 D から学習した経路情報よりも優先度が高いとします。また，本装置 B は，ネットワーク A 宛の経路情報を学習した本装置 A および本装置 C とピアを形成し，ネットワーク A 宛の経路情報を本装置 A および本装置 C のそれぞれから学習しています。本装置 A から学習した経路情報は本装置 C から学習した経路情報よりも優先度が高いとします。

この状態で第 2 優先経路を生成するように設定した場合，本装置 A および本装置 B から学習した経路を第 1 優先経路，本装置 C および本装置 D から学習した経路を第 2 優先経路とし，第 1 優先経路をフォワーディングテーブルに登録します。これによって本装置 A ではネットワーク B 宛の経路は本装置 B にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 A にルーティングします (図の (a) のケース)。

このとき，本装置 A と本装置 B との間で障害が発生し，第 1 優先経路が使用不可能になると，即座に第 2 優先経路をフォワーディングテーブルに登録し，本装置 A ではネットワーク B 宛の経路は本装置 D にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 C にルーティングします (図の (b) のケース)。

このように，本装置 A と本装置 B でインタフェース障害を検出して即座に第 2 優先経路に切り替えることで通信停止時間を短縮できます。

(3) BGP4 プロトコルによる適用例 (マルチパス経路の縮退)

コンフィグレーションコマンド options の fast-reroute パラメータが設定されている場合，マルチパス経路の縮退が高速化されます。

図 13-3 BGP4 プロトコルによる高速経路切替機能の適用例 (マルチパス経路の縮退)

(a) 経路切り替え前

(b) 経路切り替え後

この図で本装置 A は，ネットワーク B 宛の経路情報を学習した本装置 B および本装置 D とピアを形成し，ネットワーク B 宛の経路情報を本装置 B および本装置 D のそれぞれから学習しています。本装置 B から学習した経路情報と本装置 D から学習した経路情報の優先度は同一とします。また，本装置 B は，ネットワーク A 宛の経路情報を学習した本装置 A および本装置 C とピアを形成し，ネットワーク A 宛の経路情報を本装置 A および本装置 C のそれぞれから学習しています。本装置 A から学習した経路情報と本装置 C から学習した経路情報の優先度は同一とします。

この状態で BGP マルチパスが設定されている場合，本装置 A は本装置 B から学習した経路と本装置 D から学習した経路の間でマルチパスを形成しフォワーディングテーブルに登録します。また，本装置 B は本装置 A から学習した経路と本装置 C から学習した経路の間でマルチパスを形成しフォワーディングテーブルに登録します。これによって本装置 A ではネットワーク B 宛の経路は本装置 B または本装置 D にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 A または本装置 C にルーティングします (図の (a) のケース)。

このとき，本装置 A と本装置 B との間で障害が発生し，マルチパスの一方が使用不可能になると，使用不可能となったパスを即座にフォワーディングテーブルから削除し，本装置 A はネットワーク B 宛の経路はすべて本装置 D にルーティングし，本装置 B はネットワーク A 宛の経路はすべて本装置 C にルーティングします (図の (b) のケース)。

13.3 BGP4

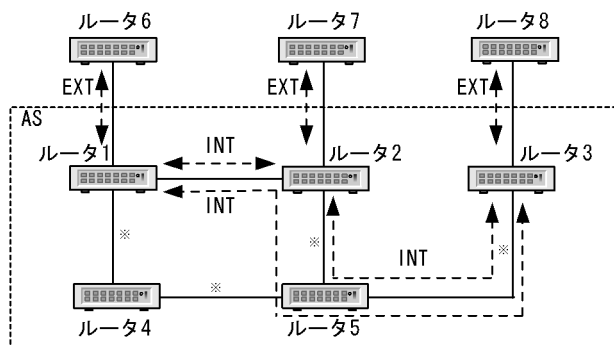
この節では BGP4 プロトコルについて説明します。

13.3.1 BGP4 の基礎

BGP4 は AS 間のルーティングプロトコルなので，扱う経路情報は宛先ネットワークへの AS パス情報（パケットが宛先のネットワークに到達するまでに通過する AS の列）で構成されます。BGP4 が動作するルータを **BGP スピーカ**といいます。この BGP スピーカはそのほかの BGP スピーカと経路情報を交換するためにピアを形成します。

(1) ピアの種類

本装置で使用されるピアの種類には外部ピアと内部ピアがあります。ネットワーク構成に合わせてピアを使用してください。外部ピアと内部ピアを次の図に示します。

図 13-4 内部ピアと外部ピア

(a) 外部ピア（エキスターナルピア）

外部ピアはエキスターナルピアとも呼ばれ，異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

「図 13-4 内部ピアと外部ピア」のルータ 1- ルータ 6 間，ルータ 2- ルータ 7 間，ルータ 3- ルータ 8 間に形成されるピアです。

(b) 内部ピア

内部の同じ AS に属する BGP スピーカ間に形成するピアです。BGP4 はピア間のコネクションを確立するために TCP(ポート 179) を使用します。このため，すべての BGP スピーカが物理的にフルメッシュで接続される必要はありませんが，内部ピアは AS 内の各 BGP スピーカ間で論理的にフルメッシュに形成されなければなりません。これは，内部ピアで受信した経路情報はそのほかの内部ピアに通知しないためです。なお，ルート・リフレクションやコンフィデレーションの機能を使用すると，この条件は緩和されます。

内部ピアには次に示す 2 種類があります。

- **インターナルピア**
  同じ AS 内に属し，物理的に直接接続された BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。IP アドレスに装置アドレスを使用する場合はルーティングピアとなります。
  「図 13-4　内部ピアと外部ピア」のルータ 1- ルータ 2 間に形成されるピアです。
- **ルーティングピア**
  同じ AS 内に属し，物理的に直接接続されない BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスはそのルータの装置アドレスか，またはルータ内のインタフェースのインタフェースアドレスのどちらかになります。
  「図 13-4　内部ピアと外部ピア」のルータ 1- ルータ 3 間，ルータ 2- ルータ 3 間に形成されるピアです。

なお，コンフィデレーション構成時は，これら三つのピアに加え，メンバー AS 間ピア (サブ AS 間ピア) が追加されます。メンバー AS 間ピアについては「13.3.6　コンフィデレーション」の項を参照してください。

(2) 装置アドレス

本装置では装置に対して IP アドレスを割り当てることができます。これを装置アドレスと呼びます。この装置アドレスを内部ピアの IP アドレスとして使用することによって，特定の物理インタフェースの状態に依存した内部ピア (TCP コネクション) への影響を排除できます。

例えば，「図 13-4　内部ピアと外部ピア」でルータ 1- ルータ 2 間の内部ピアにインタフェースの IP アドレスを使用すると，ルータ 1- ルータ 2 間に障害が発生しインタフェースが使用できない場合にルータ 1- ルータ 2 間の内部ピアは確立できません。しかし，内部ピアの IP アドレスとして装置アドレスを使用すると，ルータ 1- ルータ 2 間のインタフェースが使用できない場合でもルータ 4，ルータ 5 経由で内部ピアを確立できます。

装置アドレス使用上の注意事項

装置アドレスを使用する場合，そのアドレスへの経路情報をスタティックまたは IGP(RIP，OSPF など) でお互いに学習していなければなりません。なお，本装置は装置アドレスを直結経路情報として扱います。

ルーティングピアで非 BGP スピーカを経由する場合の注意事項

ルーティングピアで非 BGP スピーカを経由して経路情報を通知する (例えば，ルータ 2 からルータ 3 に通知する) 場合，非 BGP スピーカで IGP 経由でその経路情報を学習していなければなりません。これは該当する経路情報の通知によって通知先 BGP スピーカから入ってくる該当宛先への IP パケットが，該当する経路を学習していない非 BGP スピーカのルータで廃棄されるのを防ぐためです。例えば，「図 13-4　内部ピアと外部ピア」ではルータ 3 からルータ 5 に入ってくる IP パケットがルータ 5 で廃棄されるのを防ぐためです。

13.3.2　経路選択アルゴリズム

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最適の経路を選択します。同じ宛先への経路情報が各プロトコルでの生成によって複数存在する場合，それぞれの経路情報のプリファレンス値が比較され優先度の最も高い経路情報が有効になります。

BGP4 では，自プロトコルを使用し学習した同じ宛先への複数の経路情報から次の表に示す優先順位で一つの最適の経路を選択します。そのあと，同じ宛先への経路情報が各プロトコル (RIP，OSPF，スタティック) での経路選択によって複数存在する場合は，それぞれの経路情報のプリファレンス値が比較されて，優先度の最も高い経路情報をルーティングテーブルに設定します。

表 13-8　経路選択の優先順位

優先順位	内容
高	LOCAL_PREF 属性の値が最も大きい経路を選択します。
↑	AS_PATH 属性の AS 数が最も短い経路を選択します。
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。
	外部ピアで学習した経路，内部ピアで学習した経路の順で選択します。
	ネクストホップが最も近い（ネクストホップ解決時に使用した IGP 経路のメトリック値が最も小さい）経路を選択します。
↓	相手 BGP 識別子（ルータ ID）が最も小さい経路を選択します。
低	比較する経路が BGP4 マルチパスの関係にある場合に，学習元ピアのアドレスが若い経路を選択します。

経路選択に関連する経路情報に含まれる BGP 属性（LOCAL_PREF 属性，AS_PATH 属性，ORIGIN 属性，MED 属性，NextHop 属性）の概念を次に説明します。

経路選択上の注意事項

- AS_PATH 属性上のパスタイプ AS_SET は全体で一つの AS としてカウントします。
- コンフィグレーションコマンド bgp の compare-aspath サブコマンドに no を指定することによって，AS パス長による経路選択を無効化できます。
- MED 属性値による経路選択は，同一隣接 AS から学習した重複経路に対してだけ有効です。なお，コンフィグレーションコマンド bgp の compare-med サブコマンドに all-as を指定することによって，異なる隣接 AS から学習した重複経路に対しても有効となります。

(1) LOCAL_PREF 属性

LOCAL_PREF 属性は，同じ AS 内のルータ間で通知される属性です。同じ宛先ネットワークに対して複数の経路がある場合，LOCAL_PREF 属性は該当する宛先ネットワークに対する優先経路を示します。より大きい LOCAL_PREF 属性値を持つ経路が優先されます。

本装置で使用できる LOCAL_PREF 属性値は 0 ～ 65535 の範囲で指定します。デフォルト値は 100 です。

(a) LOCAL_PREF 属性のデフォルト値の変更

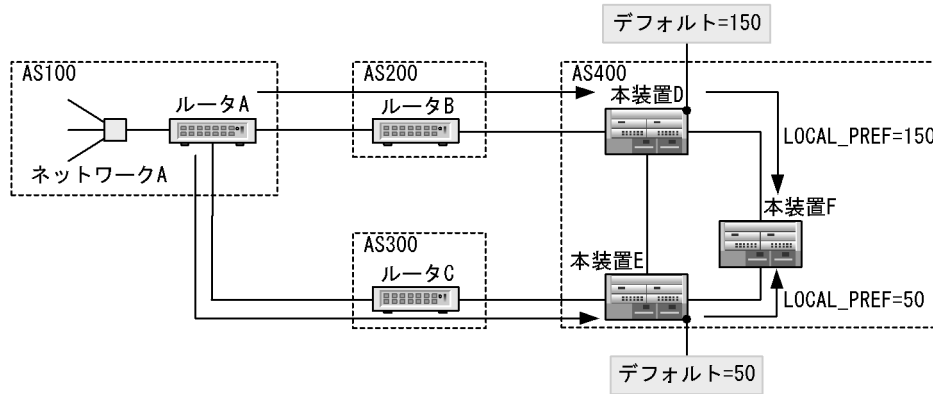
本装置ではコンフィグレーションコマンド bgp の default-localpref サブコマンドを指定して，外部ピアから自装置内に取り込む経路情報の LOCAL_PREF 属性値を変更できます。

(b) LOCAL_PREF 属性のフィルタ単位での変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の localpref サブコマンド（パラメータ）を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の LOCAL_PREF 属性を変更できます。

(c) LOCAL_PREF 属性による経路選択の例

LOCAL_PREF 属性による経路選択を次の図に示します。

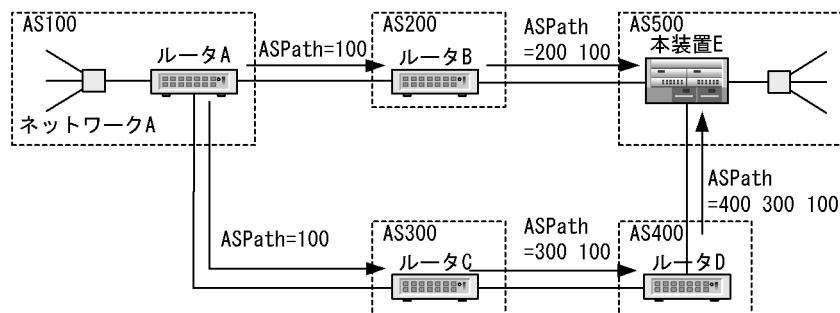
図 13-5　LOCAL_PREF 属性による経路選択

この図で，AS400 は AS200 と AS300 からネットワーク A に対する経路情報を受け取ります。本装置 D の default-localpref 値を 150 に，本装置 E の default-localpref 値を 50 に設定するとします。それによって，本装置 D は AS200 からの経路情報を本装置 F に通知するとき LOCAL_PREF 値を 150 に設定し，本装置 E は AS300 からの経路情報を本装置 F に通知するとき，LOCAL_PREF 値を 50 に設定します。本装置 F でのネットワーク A への経路情報は，本装置 D からの経路情報が本装置 E からの経路情報より大きい LOCAL_PREF 属性値を持つため，本装置 D からの経路情報 (AS200 経由の経路情報) を選択します。

（2） AS_PATH 属性

AS_PATH 属性は，経路情報の宛先ネットワークに到達するまでに通過する AS 番号のリストです。経路情報がほかの AS に通知されるとき，その経路情報の AS_PATH 属性に自 AS 番号を追加します。また，コンフィグレーションの指定 (コンフィグレーションコマンド attribute-list/route-filter の ascount サブコマンド (パラメータ) と import，export コマンドとの組み合わせ) によって複数の自 AS 番号を AS_PATH 属性に追加することもできます。これはある宛先ネットワークへの複数の経路がある場合に特定の経路を選択するのに有効です。

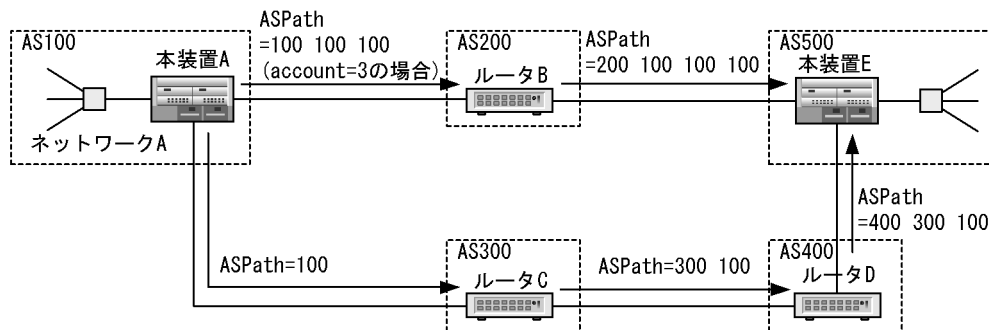
（a） AS_PATH 属性による経路選択の例

AS_PATH 属性による経路選択を次の図に示します。

図 13-6　AS_PATH 属性による経路選択

ルータ A が自 AS に存在するネットワーク A を AS200 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「200 100」を持ちます。ルータ A が自 AS 内のネットワーク A を AS300，AS400 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「400 300 100」を持ちます。したがって，AS500 の本装置 E は最も短い AS_PATH 属性を持つ AS200 経由で到達した経路を選択します。

(b) AS_PATH 属性の ascount サブコマンド (パラメータ) 使用時の経路選択

ascount サブコマンド (パラメータ) の例を次の図に示します。

図 13-7 ascount サブコマンド (パラメータ) の使用例

この図で，本装置 A が本装置 E に対し AS300 AS400 経由の経路を選択させたい場合，AS200 に通知する経路情報の AS_PATH 属性に複数の自 AS 番号を追加します。例えば，自 AS 番号を三つ追加 (ascount = 3) した場合，AS200 経由で AS500 に到達する経路情報の AS_PATH 属性は「200 100 100 100」を持ち，本装置 E は最も短い AS_PATH 属性を持つ AS300 AS400 経由で到達した経路を選択します。

(3) ORIGIN 属性

ORIGIN 属性は，経路情報の生成元を示します。ORIGIN 属性を次の表に示します。

表 13-9 ORIGIN 属性

ORIGIN 属性	内容
IGP	該当する経路が AS 内部で生成されたことを示す。
EGP	該当する経路が EGP 経由で学習されたことを示す。
Incomplete	該当する経路が上記以外の方法で学習されたことを示す。

経路選択では，同一宛先への複数の経路が存在する場合，IGP，EGP，Incomplete の順で選択します。

(a) ORIGIN 属性の変更

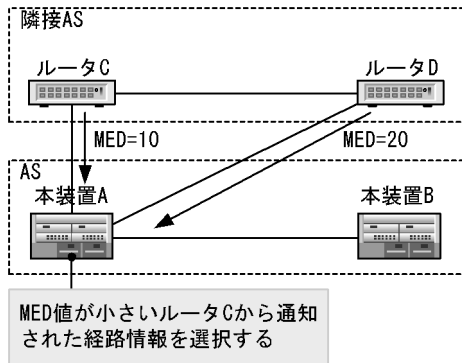
本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の origin サブコマンド (パラメータ) を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の ORIGIN 属性を変更できます。

(4) MED 属性

MED 属性は，同一の隣接 AS から学習した，ある宛先への複数の BGP4 経路の優先度を決定する属性です。より小さい MED 属性値を持つ経路情報が優先されます。コンフィグレーションコマンド bgp の compare-med サブコマンドに all-as を指定して，異なる隣接 AS から学習した BGP4 経路間の優先度選択に使用できます。

(a) MED 属性による経路選択の例

MED 属性による経路選択を次の図に示します。

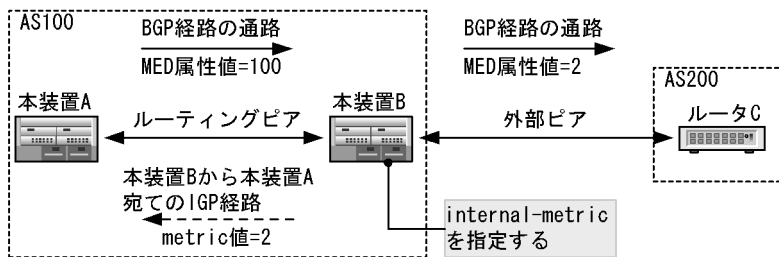
図 13-8　MED 属性による経路選択

ある宛先ネットワークに対する経路情報をルータ C は MED 属性値 10 で，ルータ D は MED 属性値 20 で本装置 A に通知しているものとします。この場合，本装置 A はルータ C から通知された経路情報を該当する宛先ネットワークへの経路として選択します。

MED 属性による経路選択はコンフィグレーション (コンフィグレーションコマンド bgp の med サブコマンド) で設定する必要があります。med サブコマンドが設定されていない場合，MED 属性による経路選択は行いません。

(b) MED 属性値の変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list または route-filter の med サブコマンド (パラメータ) を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の MED 属性値を変更できます。

また，med サブコマンド (パラメータ) に internal-metric を指定した場合，NextHop 解決に使用している IGP 経路のメトリック値を，通知する BGP4 経路の MED 属性値にすることができます。
internal-metric の使用例を次の図に示します。

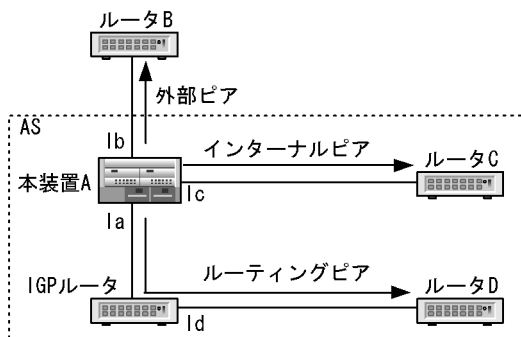
図 13-9　internal-metric の使用例

この図では本装置 A，本装置 B の間でルーティングピアを形成しています。MED 属性値 =100 で本装置 A から通知された BGP4 の経路情報を本装置 B がルータ C に通知するとき，本装置 B から本装置 A までの IGP 経路のメトリック値 =2 を MED 属性値に設定したい場合，本装置 B のエキスポート・フィルタで med サブコマンド (パラメータ) に internal-metric を指定します。

(5) NextHop 属性

NextHop 属性は，ある宛先ネットワークに到達するために使用されるネクストホップの IP アドレスです。本装置では相手 BGP スピーカに経路情報を通知する場合，NextHop 属性にピアリングに使用した自側の IP アドレスを設定します。

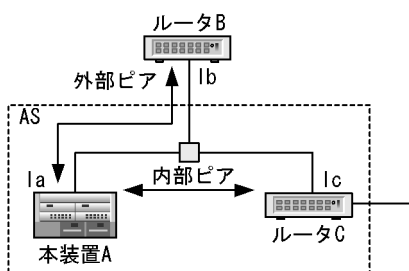
(a) NextHop 属性の設定例

通知する経路情報の NextHop 属性の設定例を次の図に示します。

図 13-10　通知する経路情報の NextHop 属性の設定例

- 外部ピアを形成するルータ B への経路情報
  NextHop 属性は本装置 A とルータ B 間のインタフェースの本装置 A 側のインタフェースアドレス Ib になります。
- 内部ピア (インターナルピア) を形成するルータ C への経路情報
  NextHop 属性は本装置 A とルータ C 間のインタフェースの本装置 A 側のインタフェースアドレス Ic になります。
- 内部ピア (ルーティングピア) を形成するルータ D への経路情報
  NextHop 属性は本装置 A と IGP ルータ間のインタフェースの本装置 A 側のインタフェースアドレス Ia になります。
  なお，ピアリングアドレスに「13.3.1　BGP4 の基礎　(2) 装置アドレス」で説明した装置アドレスを使用している場合には，装置アドレスが NextHop 属性に設定されます。

(b) NextHop 属性を書き換えない場合

ブロードキャスト型インタフェースで接続されたピア間で経路情報を通知する場合，通知する経路情報の NextHop 属性を書き換えません。ブロードキャスト型インタフェース接続での NextHop 属性の設定例を次の図に示します。

図 13-11　ブロードキャスト型インタフェース接続での NextHop 属性の設定例

本装置 A と外部ピアを形成するルータ B から通知された経路情報を，内部ピアを形成するルータ C に通知する場合，通知する NextHop 属性はルータ B から通知されたネクストホップ (Ib) のままになります。また，ルータ C から通知された経路情報をルータ B に通知する場合，通知する経路情報の NextHop 属性はルータ C から通知されたネクストホップ (Ic) のままになります。つまり，通知する経路情報のネクストホップが通知するインタフェースと同一のネットワーク上に存在する場合，NextHop 属性は書き換えません。

(c) NextHop 属性の解決

ルーティングピアから BGP4 経路情報を学習した場合，NextHop 属性で示されたアドレスへ到達するためのパスを，IGP 経路，スタティック経路，および直結経路によって解決します。BGP4 経路の NextHop へ到達可能な経路の中から，宛先のマスク長が最も長い経路を選択し，当該経路のパスを BGP4 経路のパスとして使用します。また，bgp コンフィグレーションコマンドの resolve-nexthop オプションで all を指定すると，上記の経路に加えて，BGP4 経路を NextHop の解決に使用します。

なお，NextHop を解決した経路がスタティック経路で，かつ，noinstall オプションの指定がある場合，当該 BGP4 経路を抑止します。この機能は次のような場合に利用できます。

- 宛先不明の中継トラフィックを廃棄するため，null インタフェース向けのデフォルト経路を設定してあるルータで，当該デフォルト経路によって BGP4 経路の NextHop が解決されてしまうことを防ぐために，NextHop 宛のスタティック経路を定義し，noinstall オプションを指定します。

13.3.3 コミュニティ

本装置では経路情報に付加された Community 属性を使用して，経路情報の広告範囲を制限できます。

(1) Community 属性の種類

本装置で取り扱う Community 属性の値は，次の 2 種類に分けられます。

- RFC1997 であらかじめ定義された値 (コード)
  通知された経路情報に RFC1997 であらかじめ定義された値の Community 属性が付加されている場合，その値に従い経路情報を広告します。RFC1997 で定義され，本装置で使用できる Community 属性については「表 13-10　本装置で使用できる Community 属性」を参照してください。
- コンフィグレーションのインポート・フィルタまたはエキスポート・フィルタで指定された任意の値
  通知された経路情報にコンフィグレーションのインポート・フィルタまたはエキスポート・フィルタで指定された任意の値の Community 属性が付加されている場合，コンフィグレーションに従ってその経路情報を取り込むかどうか (インポート・フィルタ時)，または広告するかどうか (エキスポート・フィルタ時) を制御します。

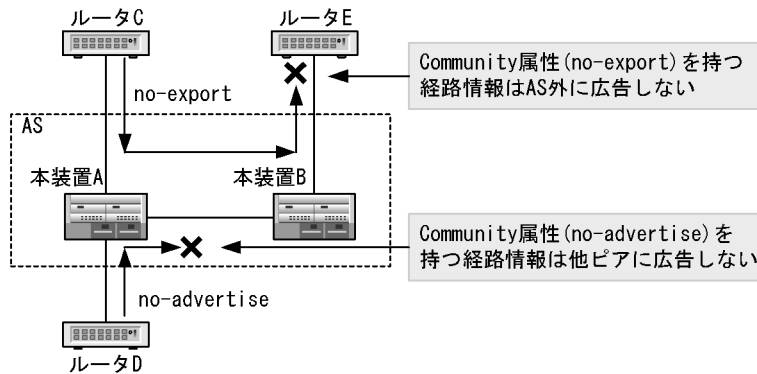
また，インポート・フィルタ，およびエキスポート・フィルタによって本装置が通知する経路情報に任意の Community 属性を付加できます。

RFC1997 で定義され，本装置で使用できる Community 属性を「表 13-10　本装置で使用できる Community 属性」に示します。また，Community 属性を持つ経路情報の広告範囲を「図 13-12　Community 属性を持つ経路情報の広告範囲」に示します。

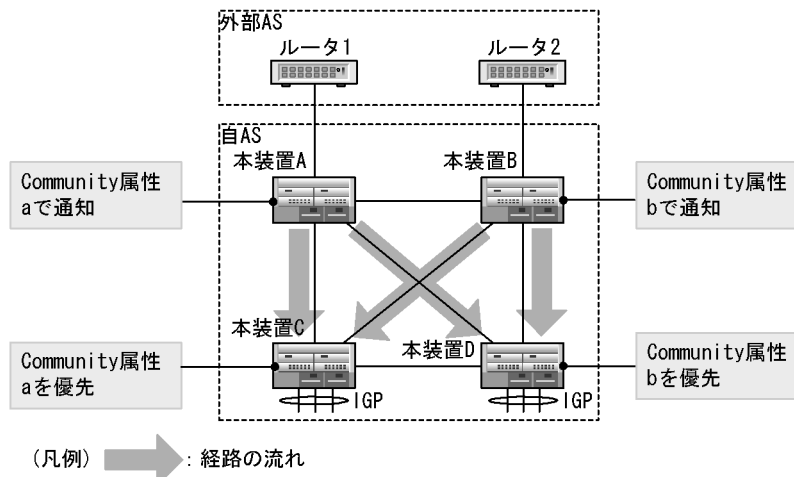
表 13-10　本装置で使用できる Community 属性

Community 属性	内容
no-export	この経路情報を AS 外に広告しません。
no-advertise	この経路情報をほかのピアに広告しません。
no-export-subconfed	• 「通常構成 (非コンフィデレーション構成) 時」 この経路情報を外部ピアに広告しません。 • 「コンフィデレーション構成時」 この経路情報を他 AS を含めたメンバー AS 外に広告しません。

注　通常構成では Community 属性 no-export と no-export-subconfed は同じ意味を持ちます。コンフィデレーション構成での community 属性の取り扱いは「13.3.6　コンフィデレーション」を参照してください。

図 13-12　Community 属性を持つ経路情報の広告範囲

(2) インポート・フィルタと Community 属性の使用例

インポート・フィルタと Community 属性の使用例を次の図に示します。

図 13-13　インポート・フィルタと Community 属性の使用例

この図で，一つの外部 AS に 2 台のルータ (本装置 A と本装置 B) が接続されているものとします。AS 外へのトラフィックの負荷分散を考慮し，本装置 C からのトラフィックは本装置 A を経由し AS 外に，本装置 D からのトラフィックは本装置 B を経由し AS 外に優先して中継するものとします。このような場合，各ルータに次のような設定をすると，負荷分散できるようになります。

1. 本装置 A から内部ピアに通知する経路情報に Community 属性 a を付加します。
   (エキスポート・フィルタで指定できます)
2. 本装置 B から内部ピアに通知する経路情報に Community 属性 b を付加します。
   (エキスポート・フィルタで指定できます)
3. 本装置 C で，受信した経路情報が Community 属性 a を持つ場合，該当する経路情報のプリファレンス値を x(x < y) に設定し，受信した経路情報が Community 属性 b を持つ場合，該当する経路情報のプリファレンス値を y(x < y) に設定します。つまり，本装置 A から通知された経路情報を優先します。
   (インポート・フィルタで指定できます)
4. 本装置 D で，受信した経路情報が Community 属性 a を持つ場合，該当する経路情報のプリファレンス値を y(x < y) に設定し，受信した経路情報が Community 属性 b を持つ場合，該当する経路情報のプリファレンス値を x(x < y) に設定します。つまり，本装置 B から通知された経路情報を優先します。

（インポート・フィルタで指定できます）

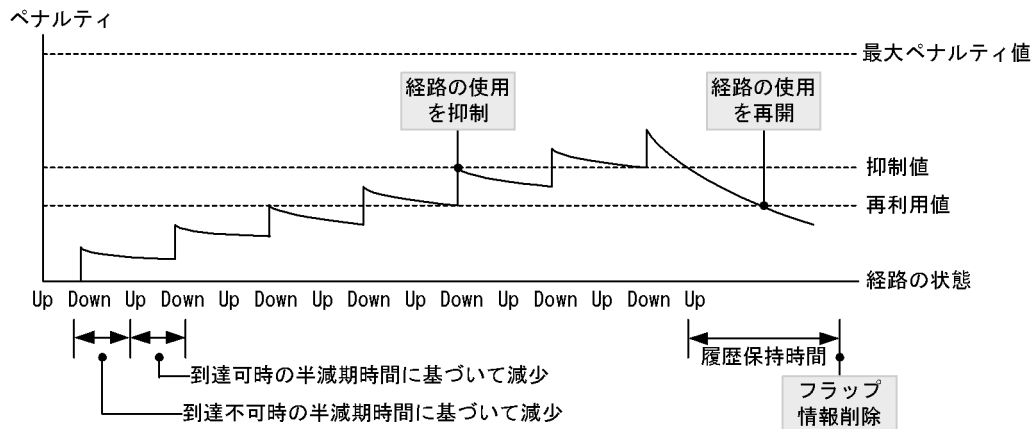
13.3.4　ルート・フラップ・ダンピング

ルート・フラップ・ダンピングは，経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。ルート・フラップ・ダンピング機能の構成要素を次の表に示します。

表 13-11　ルート・フラップ・ダンピング機能の構成要素

構成要素	内容
ペナルティ	該当する経路の使用を抑制または再利用するための動的制御変数。 経路のフラップによって増加し，時間経過とともに減少します。ペナルティの増加はフラップ（到達不可への変化）当たり 1 固定で，ペナルティの減少は半減期時間に基づきます。
抑制値	ペナルティが本値以上の場合，該当する経路の使用を抑制します。
再使用値	ペナルティが本値以下の場合，該当する経路の使用を開始します。
最大ペナルティ値	累積されるペナルティの最大値。
到達可時の半減期時間	該当する経路が到達可状態である場合に，ペナルティが半減（50%）するために要する時間。
到達不可時の半減期時間	該当する経路が到達不可状態である場合に，ペナルティが半減（50%）するために要する時間。
履歴保持時間	ルート・フラップ情報を保持する時間。この値は最後にフラップが発生してからの経過時間に基づきます。

ルート・フラップ・ダンピングの動作概念を次の図に示します。

図 13-14　ルート・フラップ・ダンピングの動作概念

13.3.5　ルート・リフレクション

ルート・リフレクションは，AS 内でピアを形成する内部ピアの数を減らすための方法です。BGP4 は，内部ピアで配布された経路情報をそのほかの内部ピアに配布しません。このため，内部ピアは AS 内の各 BGP スピーカ間で論理的にフルメッシュに形成されなければなりません。ルート・リフレクションはこの制限を緩和し，内部ピアで配布された経路情報をほかの内部ピアに再配布して，AS 内の内部ピアの数を減らします。

(1) ルート・リフレクションの概念と経路情報の流れ

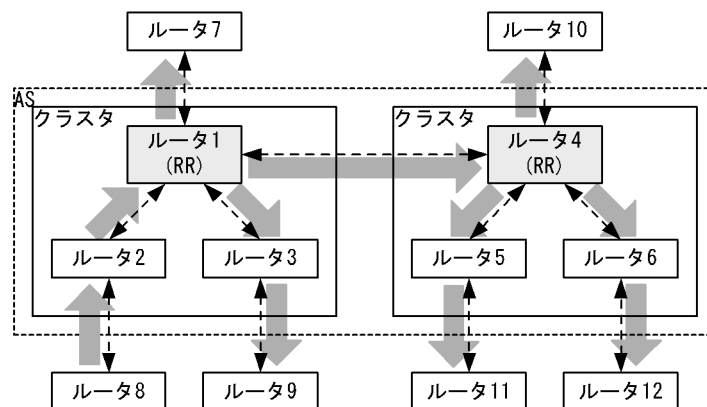
ルート・リフレクションはルート・リフレクタ (RR) とそのルート・リフレクタに対するクライアントでクラスタを形成します。クラスタ内に複数のルート・リフレクタを持つこともできます。1AS 内のそのほかの BGP スピーカをノンクライアントと呼びます。

ルート・リフレクタはクラスタ内のクライアントから受信した update メッセージをすべてのノンクライアントおよびクラスタ内のほかのクライアントに配布します。また，ルート・リフレクタはノンクライアントから受信した update メッセージをクラスタ内のすべてのクライアントに配布します。これによって，クラスタ内のクライアントからノンクライアントに対する内部ピアとクラスタ内のクライアント間の内部ピアを不要とします。

なお，外部ピアから配布された経路情報および外部ピアへ配布する経路情報の取り扱いは通常の動作と同じです。

(2) クラスタ内に一つのルート・リフレクタを置く場合

クラスタ内に一つのルート・リフレクタを置く例を次の図に示します。

図 13-15　クラスタ内に一つのルート・リフレクタを置く例

（凡例）　ルータ1，ルータ4：ルート・リフレクタ (RR)
ルータ2，ルータ3：ルータ1に対するクライアント
ルータ5，ルータ6：ルータ4に対するクライアント
: ピア
: 経路情報の流れ

ルータ 1(ルート・リフレクタ) とルータ 2，ルータ 3(クライアント) でクラスタを形成しています。また，ルータ 4(ルート・リフレクタ) とルータ 5，ルータ 6(クライアント) でクラスタを形成しています。ルータ 2 からルータ 1 に通知された経路情報は，ほかのクライアント (ルータ 3) とすべてのノンクライアント (ルータ 4) に配布されます。また，ルータ 1 からルータ 4 に通知された経路情報は，すべてのクライアント (ルータ 5，ルータ 6) に配布されます。

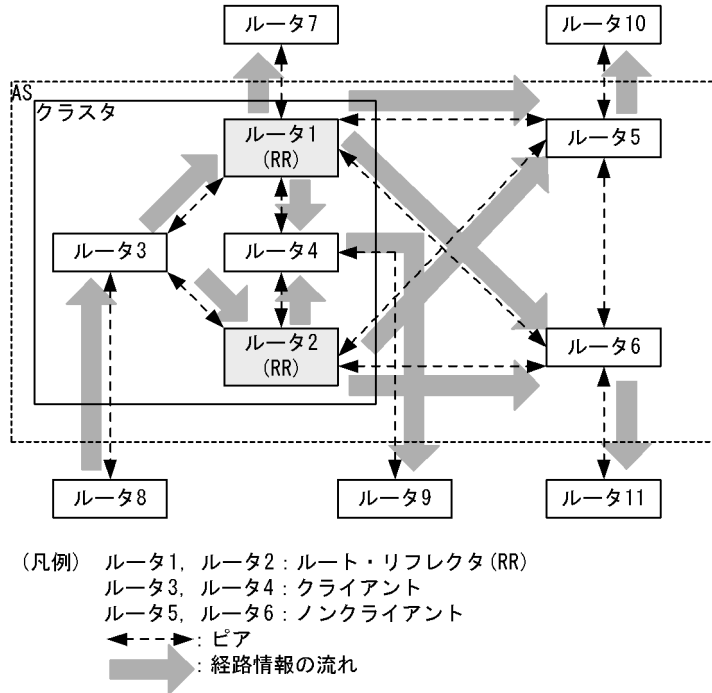
(3) クラスタ内に複数のルート・リフレクタを置く場合

クラスタは，一つ以上のルート・リフレクタを持つことができます。複数のルート・リフレクタを持つことによって，一方のルート・リフレクタが障害となった場合にもルート・リフレクションの機能の停止を防ぐことができます。

それぞれのルート・リフレクタは，クライアントおよびノンクライアントと内部ピアを形成します。それぞれのルート・リフレクタは，「図 13-15　クラスタ内に一つのルート・リフレクタを置く例」で説明した通り，クライアントまたはノンクライアントから通知された経路情報を再配布します。これによって，一

方のルート・リフレクタが障害となった場合にも，他方のルート・リフレクタの再配布によって経路情報の通知ができるようにしています。なお，クラスタ内に複数のルート・リフレクタがある場合，それぞれのルート・リフレクタは同一のクラスタ ID(コンフィグレーションコマンド bgp の clusterid サブコマンド) を設定する必要があります。

ルート・リフレクタの冗長構成の例を次の図に示します。

図 13-16　ルート・リフレクタの冗長構成の例

クラスタ内には二つのルート・リフレクタ (ルータ 1 とルータ 2) が存在しています。それぞれのルート・リフレクタはクライアントであるルータ 3，ルータ 4 およびノンクライアントであるルータ 5，ルータ 6 と内部ピアを形成します。例えば，クライアントであるルータ 3 から通知された経路情報は，それぞれのルート・リフレクタ (ルータ 1 およびルータ 2) でクライアントであるルータ 4 とノンクライアントであるルータ 5，ルータ 6 に再配布します。一方のルート・リフレクタが障害となった場合にも，他方のルート・リフレクタの再配布によって経路情報は通知されます。なお，AS 内にはクラスタに属さない BGP スピーカ (ルータ 5，ルータ 6) が共存することもできます。

(4) ルート・リフレクション構成上の注意事項

ルート・リフレクション構成時はルート・リフレクタ (RR) で，該当する AS から同 AS に経路広告するためのエキスポート・フィルタを定義してください。この定義がない場合，経路はリフレクトされません。

13.3.6　コンフィデレーション

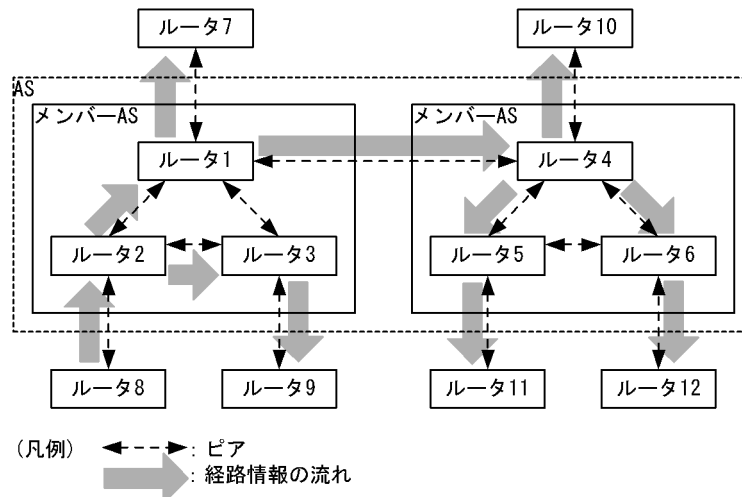
コンフィデレーションは，ルート・リフレクタと同様に AS 内でピアを形成する内部ピアの数を減らすためのもう一つの方法です。コンフィデレーションは，AS を複数のメンバー AS(サブ AS) に分割して，AS 内のピア数を減らします。

(1) コンフィデレーションの概念と経路情報の流れ

コンフィデレーションは AS を複数のメンバー AS(サブ AS) に分割します。メンバー AS 内の BGP ス

ピーカはフルメッシュに内部ピアを形成しなければならず，通常の内部ピアの取り扱いと同様です。メンバー AS 間は通常の外部ピアと同様にピアを形成すればよく，メンバー AS 間の各 BGP スピーカでフルメッシュにピアを形成する必要はありません。これによって AS 内のピア数を減らします。なお，本装置ではメンバー AS 間のピアをメンバー AS 間ピアと呼びます。

コンフィデレーション構成での経路情報の流れを次の図に示します。

図 13-17　コンフィデレーション構成での経路情報の流れ

ルータ 1，ルータ 2，およびルータ 3 でメンバー AS(サブ AS) を形成しています。また，ルータ 4，ルータ 5，およびルータ 6 でメンバー AS(サブ AS) を形成しています。ルータ 8 から通知された経路情報はルータ 2 によってメンバー AS 内のほかの BGP スピーカ (ルータ 1，ルータ 3) に配布されます。ルータ 2 からルータ 1 に通知された経路情報はほかのメンバー AS(ルータ 4) に配布されます。さらに，ルータ 1 からルータ 4 に通知された経路情報は，メンバー AS 内のほかの BGP スピーカ (ルータ 5，ルータ 6) に配布されます。これによって，AS 内のすべての BGP スピーカに経路情報を配布します。

(2)　コンフィデレーション構成での経路選択

コンフィデレーション構成での経路選択は，ピア種別 (メンバー AS 間ピア) の追加によって通常構成 (非コンフィデレーション構成) での経路選択と一部異なります。通常構成では「外部ピアで学習した経路，内部ピアで学習した経路の順」で選択しますが，コンフィデレーション構成では「外部ピアで学習した経路，メンバー AS 間ピアで学習した経路，内部ピアで学習した経路の順」で選択します。

コンフィデレーション構成での経路選択の優先順位を次の表に示します。

表 13-12　経路選択の優先順位

優先順位	内容
高	LOCAL_PREF 属性の値が最も大きい経路を選択します。
↑	AS_PATH 属性の AS 数が最も短い経路を選択します。
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。
	外部ピアで学習した経路，メンバー AS 間ピアで学習した経路，内部ピアで学習した経路の順で選択します。
	ネクストホップが最も近い (ネクストホップ解決時に使用した IGP 経路のメトリック値が最も小さい) 経路を選択します。

優先順位	内容
↓	相手 BGP 識別子 (ルータ ID) が最も小さい経路を選択します。
低	比較する経路が BGP4 マルチパスの関係にある場合に，学習元ピアのアドレスが若い経路を選択します。

経路選択上の注意事項

- AS_PATH 属性上のパスタイプ AS_SET は，全体で一つの AS としてカウントします。
- AS_PATH 属性上のパスタイプ AS_CONFED_SET は，AS パス長には含まれません。
- コンフィグレーションコマンド bgp の compare-aspath サブコマンドに no を指定することで，AS パス長による経路選択を無効化できます。
- MED 属性値による経路選択は，同一隣接 AS から学習した重複経路に対してだけ有効です。なお，コンフィグレーションコマンド bgp の compare-med サブコマンドに all-as を指定することで，異なる隣接 AS から学習した重複経路に対しても有効となります。

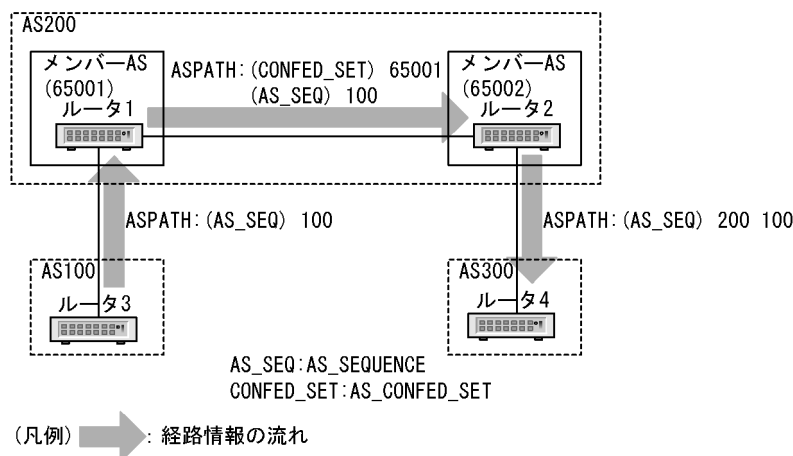
(3) コンフィデレーション構成での BGP 属性の取り扱い

コンフィデレーション構成での BGP 属性の取り扱いは，通常構成 (非コンフィデレーション構成) での BGP 属性の取り扱いとほぼ同様ですが，AS_PATH 属性，および Community 属性について一部動作が異なります。なお，メンバー AS 間ピアでの BGP 属性の取り扱いは，内部ピアでの BGP 属性の取り扱いと同様です。

(a) コンフィデレーション構成での AS_PATH 属性の取り扱い

コンフィデレーション構成での AS_PATH 属性の取り扱いは，メンバー AS 間ピアに経路情報を通知するとき，AS_PATH 属性にパスタイプ AS_CONFED_SET で自メンバー AS 番号を追加します。また，ほかの AS(外部ピア) に経路情報を通知するとき，AS_PATH 属性からパスタイプ AS_CONFED_SET を取り除き，パスタイプ AS_SEQUENCE で自 AS 番号を追加します。そのほかの AS_PATH 属性の取り扱いは，通常構成と同様です。

AS_PATH 属性の取り扱いを次の図に示します。

図 13-18　AS_PATH 属性の取り扱い

ルータ 1 は AS100 から通知された ASPATH:(AS_SEQUENCE) 100 の経路情報をほかのメンバー AS であるルータ 2 に配布するとき，AS_PATH 属性にパスタイプ AS_CONFED_SET で自メンバー AS 番号 (65001) を追加します。ルータ 2 はルータ 1 から通知された ASPATH:(AS_CONFED_SET) 65001,

(AS_SEQUENCE)100 の経路情報を AS300 に配布するとき，AS_PATH 属性のパスタイプ AS_CONFED_SET を取り除き，パスタイプ AS_SEQUENCE で自 AS 番号 (200) を追加します。

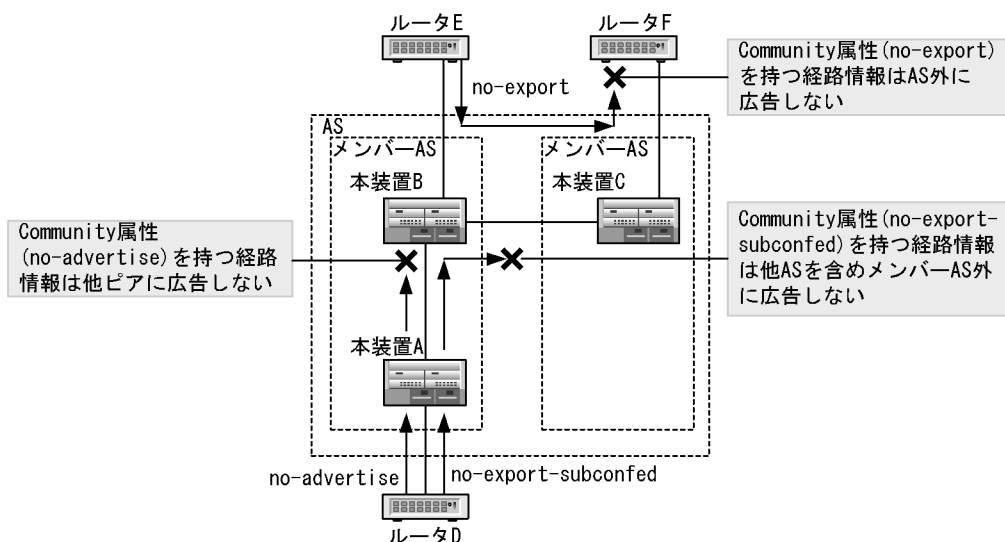
(b) コンフィデレーション構成での Community 属性の取り扱い

コンフィデレーション構成では RFC1997 で定義される Well-known Community について，次のように取り扱います。そのほかの Community の取り扱いは，通常構成と同様です。

RFC1997 で定義される Well-Known Community を「表 13-13　RFC1997 で定義される Well-Known Community」に示します。また，Community 属性を持つ経路情報の広告範囲を「図 13-19　Community 属性を持つ経路情報の広告範囲」に示します。

表 13-13　RFC1997 で定義される Well-Known Community

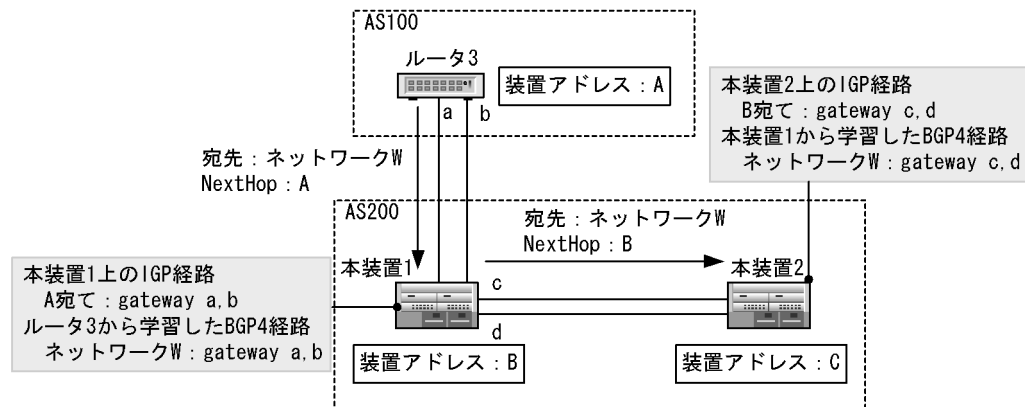
Community 属性	内容
no-export	この経路情報を AS 外に広告しません。
no-advertise	この経路情報をほかのピアに広告しません。
no-export-subconfed	この経路情報を，他 AS を含めてメンバー AS 外に広告しません。

図 13-19　Community 属性を持つ経路情報の広告範囲

13.3.7　BGP4 マルチパス

BGP4 マルチパスは，一つの宛先ネットワークに対し複数の経路 (パス) を生成し，トラフィックの負荷分散を実現します。本装置での BGP4 経路のマルチパス生成の概念を次に示します。

(1) IGP 経路のマルチパス化による BGP4 経路のマルチパス

本装置は BGP4 経路のネクストホップ解決を IGP 経路に基づいて行います。ネクストホップ解決時，BGP4 経路の NextHop 属性値に対応する IGP 経路がマルチパス化されている場合は BGP4 経路もマルチパス化されます。マルチパス生成の概念を次の図に示します。

図 13-20　IGP 経路のマルチパス化による BGP4 経路マルチパス化の概念

各ルータ間は物理的に 2 本のインタフェースが接続されているものとします。各ルータ間のピアリングは装置自体に付与されたアドレスを使用するように構成します。本装置ではコンフィグレーションコマンド local-address によって，装置自体にアドレスを付与できます。また，コンフィグレーションコマンド externalpeeras/internalpeeras/routingpeeras(bgp モード）の lcladdr サブコマンドを使用して，ピアリングの自側アドレスに装置アドレスの使用を指定できます。なお，外部ピアおよび内部ピア（インターナルピア）で lcladdr サブコマンドを使用する場合は，コンフィグレーションコマンド peer(bgp externalpeeras/bgp internalpeeras モード）の multihop サブコマンドも合わせて指定してください。

AS100 から本装置 1 に通知された BGP4 経路（宛先：ネットワーク W，NextHop：A）は，ネクストホップ解決時に IGP 経路を参照します。NextHopA 宛ての IGP 経路のゲートウェイが「a」および「b」となっていることによって，BGP4 経路のゲートウェイも「a」および「b」になります。同様に，本装置 1 から本装置 2 に通知された BGP4 経路（宛先：ネットワーク W，NextHop：B）は，NextHopB 宛ての IGP 経路のゲートウェイが「c」および「d」となっていることによって，BGP4 経路のゲートウェイも「c」および「d」になります。

IGP 経路のマルチパス化に伴う BGP4 マルチパスの注意事項

本装置でマルチパス化を行える IGP 経路はスタティック経路および OSPF 経路です。スタティック経路のマルチパス化の概念については「12.3.1　スタティックルーティング」を，OSPF 経路のマルチパス化の概念については「(2)　イコールコストマルチパス」の項を参照してください。

(2)　複数のピアから学習した BGP4 経路のマルチパス

本装置はコンフィグレーションコマンド bgp の multipath サブコマンド，およびコンフィグレーションコマンド options の max-paths パラメータを定義して，同一隣接 AS と接続された複数のピアから学習したタイブレーク状態にある同一宛先への BGP4 経路をマルチパス化できます。また，コンフィグレーションコマンド bgp の multipath-option サブコマンドに all-as を指定して，異なる隣接 AS から学習した，BGP4 経路をマルチパス化できます。タイブレーク条件を次の表に示します。

表 13-14　タイブレーク条件

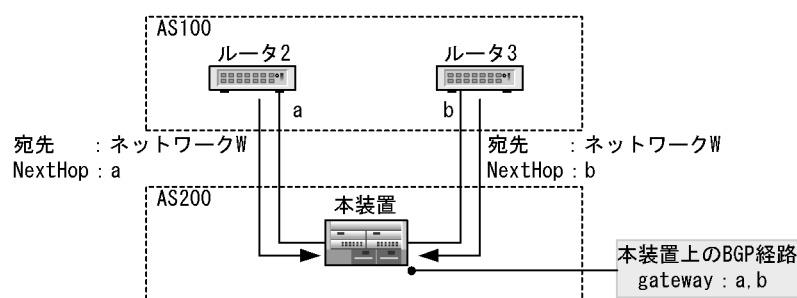
条件	備考
LOCAL_PREF 属性の値が等しい。	-
AS_PATH 属性の取り扱い属性の AS 数が等しい。	AS_PATH 属性の取り扱い属性上のパスタイプ AS_SET は，全体で一つの AS としてカウントします。 AS_PATH 属性の取り扱い属性上のパスタイプ AS_CONFED_SET は，AS パス長には含まれません。

条件	備考
ORIGIN 属性の値が等しい。	-
MED 属性の値が等しい。	MED 属性値によるタイブレーク条件は，同一隣接 AS から学習した重複経路に対してだけ有効になります。なお，コンフィグレーションコマンド bgp の compare-med サブコマンドに all-as を指定すると，異なる隣接 AS から学習した重複経路に対しても有効になります。
同一ピアタイプ (外部ピア，メンバー AS 間ピア，内部ピア) で学習している。	-
ネクストホップが等しい (ネクストホップ解決時に使用した IGP メトリックが等しい)。	-

(凡例) - : 該当しない

注 コンフィグレーションコマンド bgp の compare-aspath サブコマンドに no を指定することで，AS パス長によるタイブレーク条件を無効化できます。

複数のピアから学習した BGP4 経路マルチパス化の概念を次の図に示します。

図 13-21 複数のピアから学習した BGP4 経路マルチパス化の概念

AS100 のルータ 2，およびルータ 3 から本装置 1 に通知された BGP4 経路 (ルータ 2 の経路 : 宛先 ネットワーク W，NextHop a，ルータ 3 の経路 : 宛先 ネットワーク W，NextHop b) がタイブレーク状態である場合，本装置 1 は各 BGP4 経路が持っている NextHop 属性を基にゲートウェイを生成します。「図 13-21 複数のピアから学習した BGP4 経路マルチパス化の概念」の例では，ゲートウェイは「a」および「b」となります。なお，該当する BGP4 経路を本装置 1 からそのほかの BGP4 ピアに広告する場合は，今まで示した 2 経路のうち最優先経路を広告します。

13.3.8 サポート機能のネゴシエーション

サポート機能のネゴシエーション (Capability Negotiation) は，BGP4 コネクション確立時の OPEN メッセージに Capability 情報を付加することによって，ピア間で使用できる機能をネゴシエーションする機能です。お互いに広告した Capability 情報で一致する (お互いにサポートする) 機能を該当するピアで使用できます。

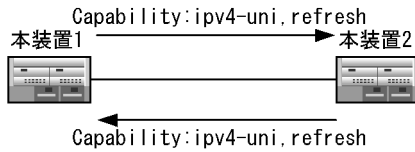
本装置では，Capability 関連パラメータをコンフィグレーションで定義した場合，OPEN メッセージに Capability 情報を付加します。Capability 関連パラメータをコンフィグレーションで定義していない場合，OPEN メッセージに Capability 情報を付加しません。Capability 情報を持たない OPEN メッセージで確立した BGP4 コネクションは，「IPv4-Unicast 経路の送受信」だけを行います。

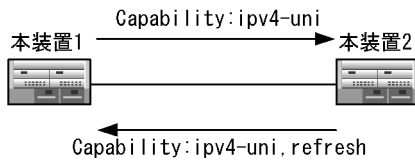
ネゴシエーションできる機能を「表 13-15 ネゴシエーションできる機能」に示します。また，ネゴシエーションの動作概念を「図 13-22 ネゴシエーションの動作概念」に示します。

表 13-15　ネゴシエーションできる機能

機能名称	サブコマンド	内容
IPv4-Unicast 経路の送受信	ipv4-uni	IPv4-Unicast 経路を該当するピア間で送受信します。
ルート・リフレッシュ	refresh	ルート・リフレッシュ機能を使用します。
ルート・リフレッシュ (Capability Code 128)	refresh-128	Capability Code に 128 を使用する BGP4 ピアとルート・リフレッシュ機能を使用します。
グレースフル・リスタート	graceful-restart	グレースフル・リスタート機能を使用します。

図 13-22　ネゴシエーションの動作概念

●お互いに同一のCapability情報を広告した場合の例

注　ピア間でIPv4-Unicast経路の送受信，およびルート・リフレッシュ機能が使用できる

●お互いに異なるCapability情報を広告した場合の例

注　ピア間でIPv4-Unicast経路の送受信だけが使用できる

13.3.9　ルート・リフレッシュ

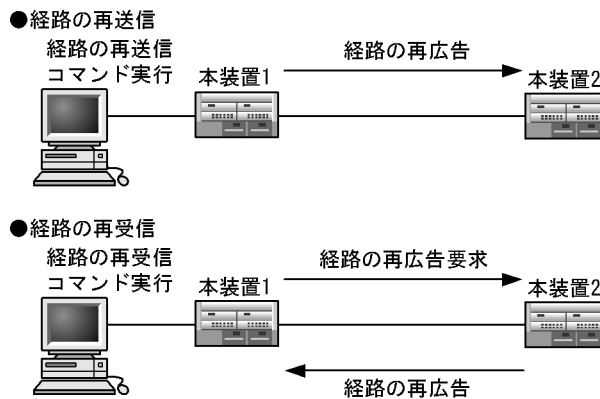
ルート・リフレッシュ機能は，変化が発生した経路だけを広告することを基本とする BGP4 で，すでに広告された経路を強制的に再広告させる機能です。

ルート・リフレッシュ機能には，自装置側から経路を再広告する機能と BGP4 ピアである相手装置側から経路を再広告させる機能があります。また，再広告の経路種別を選択できます。この機能は，clear ip bgp コマンドで実行されます。

ルート・リフレッシュ機能を「表 13-16　ルート・リフレッシュ機能」に示します。また，ルート・リフレッシュ機能の動作概念を「図 13-23　ルート・リフレッシュ機能の動作概念」に示します。

表 13-16　ルート・リフレッシュ機能

機能種別	経路種別	再広告方向
IPv4-Unicast 経路の再送信	IPv4 ユニキャスト経路	自装置側よりピアリングされた相手装置に経路を再広告します。
IPv4-Unicast 経路の再受信		ピアリングされた相手装置側より自装置に経路を再広告させます。

図 13-23 ルート・リフレッシュ機能の動作概念

(1) ルート・リフレッシュ使用時の注意事項

相手装置側から経路を再送信するには，ピアリングされた両ルータがルート・リフレッシュ機能をサポートしている必要があります。ルート・リフレッシュ機能を使用するためには，BGP4 ピア確立時にルート・リフレッシュ機能の使用を両ルータ間でネゴシエーションしておく必要があります。

本装置では，コンフィグレーションコマンド bgp の refresh サブコマンドを指定することでルート・リフレッシュ機能の使用を指定します。また，本装置のルート・リフレッシュ機能は RFC2918 に準拠しています。ルート・リフレッシュ機能をサポートするそのほかの装置によっては，ネゴシエーションで使用するルート・リフレッシュ用の Capability code(値 =2) です。なお，ほかのベンダによって RFC2434 で定義されているプライベートなコードである Capability code(値 =128 ～ 255) を使用されることがあります。

本装置と他装置間でルート・リフレッシュ機能を使用するときは注意してください。

13.3.10 TCP MD5 認証

本装置は，RFC2385(TCP MD5 認証による BGP セッション保護) に準拠しています。TCP MD5 認証機能によって，BGP4 コネクションで受信した TCP セグメントが正当な送信元 (ピア) から送信されてきたことを保証できます。TCP MD5 認証はピアごとに指定できます。ピアとの BGP4 コネクションに TCP MD5 認証を適用する場合，コンフィグレーションコマンド bgp の authmd5 サブコマンドで認証キーを指定します。なお，認証キーは該当するピア間で一致させる必要があります。一致していない場合は該当するピア間の BGP4 コネクションが確立しません。

13.3.11 グレースフル・リスタート

(1) 概要

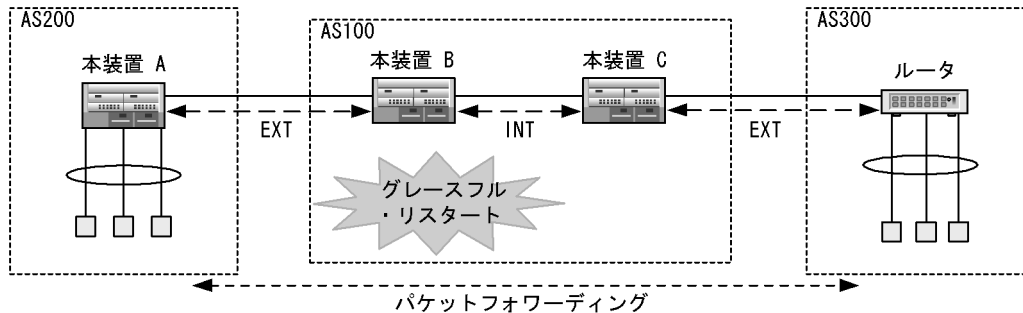
グレースフル・リスタートは，装置の BCU が系切替したり，運用コマンドなどによりルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機能です。グレースフル・リスタート機能一般については，「12.8 グレースフル・リスタートの概要」をご参照ください。

BGP4 では，グレースフル・リスタートによって BGP4 の再起動を行う装置のことをリスタートルータといいます。また，グレースフル・リスタートを補助する隣接装置をレシーブルータといいます。

SB-7800S では，リスタートルータの機能とレシーブルータの機能をサポートしています。

SB-5400S では，レシーブルータの機能だけをサポートしています。

本装置でのグレースフル・リスタートの例を次の図に示します。

図 13-24　グレースフル・リスタートの例

（凡例） INT：内部ピア（装置アドレスをピアアドレスとするルーティングピア）
　　　　EXT：外部ピア（直接接続されたインタフェースのアドレスをピアアドレスに使用する）
注　AS100内では，IGPによって装置アドレス宛ての経路情報を交換する

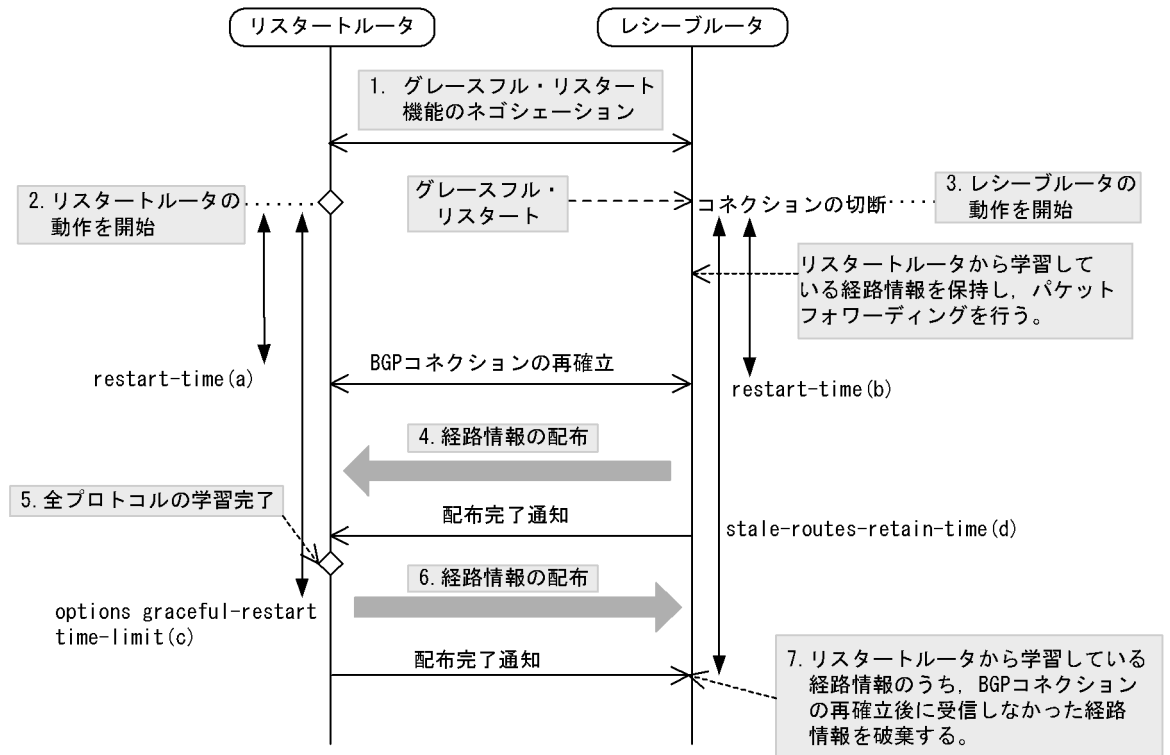
AS100 の本装置 B，本装置 C は，装置アドレスをピアアドレスとするルーティングピアの BGP コネクションを確立しており，本装置 B は AS200 の本装置 A と，また本装置 C は AS300 のルータと，それぞれインタフェースのアドレスをピアアドレスとする外部ピアの BGP コネクションを確立しているとします。それぞれの BGP コネクションでは，グレースフル・リスタート機能のネゴシエーションが成立しているとします。本装置 B がグレースフル・リスタートしたとき，当該装置との BGP コネクションを持っている本装置 A，および本装置 C はレシーブルータとして動作し，本装置 B を経由するパケット・フォワーディングを停止しないで継続します。また，本装置 B は PSU によって，パケットの転送処理を継続します。これによって，本装置 B を経由するエンド・エンドの通信を維持しつづけることができます。

以下に BGP4 のグレースフル・リスタートが正しく動作するための条件を示します。以下の条件を満たさない場合，通常のリスタート動作となって，通信が停止します。

- グレースフル・リスタートを実施する装置と，レシーブルータの役割を実行する装置との BGP コネクションで，グレースフル・リスタート機能のネゴシエーションが成立していること。
- グレースフル・リスタートを実施する装置は，リスタートルータとして動作する設定になっていること。本装置でグレースフル・リスタートを実施するときは，コンフィグレーションコマンド options で graceful-restart パラメータを設定する必要があります。また，コンフィグレーションコマンド bgp の graceful-restart サブコマンドで，mode restart または mode both パラメータが設定されている必要があります。
- レシーブルータの役割を実行する装置は，レシーブルータとして動作する設定になっていること。本装置をレシーブルータとして動作させるときは，コンフィグレーションコマンド bgp の graceful-restart サブコマンドで，mode receive または mode both パラメータが設定されている必要があります。

(2) グレースフル・リスタートの動作手順

BGP4 によるグレースフル・リスタートの動作シーケンスを次の図に示します。

図 13-25　グレースフル・リスタートのシーケンス

1. グレースフル・リスタートするルータと，その隣接ルータの間で，BGP コネクションを確立するときにグレースフル・リスタート機能のネゴシエーションを行い，グレースフル・リスタートを実施する準備をします。
2. ルータがグレースフル・リスタートすると，リスタートルータの動作を開始します。
3. 隣接ルータは，BGP のコネクションが切断したとき，レシーブルータの動作を開始して，リスタートルータから学習している経路情報を保持し，パケットのフォワーディングを継続します。
4. BGP コネクションが再確立すると，最初にレシーブルータからリスタートルータへ経路情報を配布します。
5. リスタートルータで，グレースフル・リスタートを実行しているすべてのプロトコルの学習が完了すると，リスタートルータからレシーブルータへ経路情報を配布します。
6. 5. と同じ。
7. 最後にレシーブルータは，リスタートルータから学習している経路情報のうちで，BGP コネクションの再確立後に受信しなかった，古い経路情報を破棄します。

(3)　リスタートルータの機能【SB-7800S】

(a)　動作契機

以下に，本装置で BGP4 のリスタートルータの機能が動作する契機を示します。

- BCU が系切替したとき。
- ユニキャストルーティングプログラムが再起動したとき。

(b)　リスタートルータの機能

グレースフル・リスタートの開始後に，BGP コネクションが再確立するまでの待ち時間の上限を，コンフィグレーションコマンド bgp の restart-time サブコマンドの指定に従って監視します (「図 13-25　グレースフル・リスタートのシーケンス」の (a))。この時間内に BGP コネクションが再確立しない場合，リ

スタートルータは当該レシーブルータからの経路情報配布を待たずに，自ルータからの経路情報配布を開始します。これによって，不安定な状態とみられる当該レシーブルータが経路収束へ影響することを回避します。

リスタートルータが経路情報の受信完了を待ち，経路配布を開始する時間の上限は，options コマンドの graceful-restart time-limit パラメータの指定値に従います (「図 13-25　グレースフル・リスタートのシーケンス」の (c))。

各パラメータを設定する場合は，一般に次のようにしてください。

- bgp graceful-restart restart-time を，系切替所要時間 + コネクション確立時間よりも長く設定する。
  BGP ピアのコネクションを再確立するには，系切替が完了して IP インタフェースの Up/Down が確認できるようになっている必要があります。このため，bgp graceful-restart restart-time を，系切替所要時間 + コネクション確立時間よりも長く設定してください。系切替所要時間については，「12.8　グレースフル・リスタートの概要 表 12-30　系切替所要時間の目安値」を参照してください。ピアのコネクション確立にかかる時間は，構成によって異なりますが，目安として 30 秒を用いてください。
- ルーティングピアを使用している場合，bgp graceful-restart restart-time を，OSPF・OSPFv3・IS-IS のリスタート時間 + コネクション確立時間よりも長く設定する。
  BGP 経路情報の NextHop 属性を IGP 経路によって解決する構成では，BGP ピアのコネクションを再確立するために IGP 経路が必要になります。このため，bgp graceful-restart restart-time を，IGP のリスタート時間 + コネクション確立時間よりも長く設定してください。
- options graceful-restart time-limit は bgp graceful-restart restart-time より大きい値を設定する。
  BGP ピアのコネクションの再確立が最も遅い場合は，bgp graceful-restart restart-time の経過後に BGP ピアからの経路学習を開始します。リスタートルータが経路配布を開始する前に経路学習・フォワーディングテーブルの更新が完了するようにするため，options graceful-restart time-limit の指定は restart-time より 60 秒程度長い時間を設定してください。なお，目安の設定値は，経路数および隣接ピア数に依存します。

また，BGP 経路情報の NextHop 属性を IGP 経路によって解決する構成では，次のように設定してください。

- IGP の restart-time は bgp の restart-time より小さい値を設定

(c) グレースフル・リスタートが失敗するケース

以下に，BGP4 のグレースフル・リスタートが失敗するケースを示します。

- グレースフル・リスタートを開始してから restart-time の時間が経過しても，隣接装置との間で BGP コネクションが再確立しなかった場合，当該ピア装置を経由する通信が停止します。
- 本装置のグレースフル・リスタート中に，レシーブルータ機能を実行するピア装置がリスタートした場合，当該ピア装置を経由する通信が停止します。
- レシーブルータ機能を実行するピア装置が，グレースフル・リスタートの開始前に，本装置から学習した経路情報を保持できなかった場合，当該ピア装置を経由する通信が停止します。
- グレースフル・リスタートの開始後に，すべてのレシーブルータへの経路情報の配布が完了する前に，BGP コネクションが再び切断した場合，当該ピア装置を経由する通信が停止します。
- グレースフル・リスタートの開始後に，レシーブルータ機能を実行するピア装置から学習した経路数が学習経路数制限機能による上限値を超え，BGP コネクションが再び切断した場合，当該ピア装置を経由する通信が停止します。

（4） レシーブルータの機能

（a） 動作契機

以下に，本装置で BGP4 のレシーブルータの機能が動作する契機を示します。

- BGP コネクションが確立しているピアから，NOTIFICATION メッセージを受信せずに，当該コネクションが使用している TCP セッションの切断を検出したとき
- BGP コネクションが確立しているピアから，新規の TCP セッションが接続され，OPEN メッセージを受信したとき

（b） レシーブルータの機能

グレースフル・リスタートの開始後に，BGP コネクションが再確立するまでの待ち時間の上限を，コンフィグレーションコマンド bgp の restart-time サブコマンドの指定に従って監視します (「図 13-25　グレースフル・リスタートのシーケンス」の (b))。この時間内に BGP コネクションが再確立しない場合，レシーブルータは，リスタートルータから学習している経路情報を破棄して，リスタートルータを経由するパケット・フォワーディングを停止します。

restart-time の値は，グレースフル・リスタート機能のネゴシエーションを行うときに，ピアへ通知されます。本装置では，ピアから通知された restart-time の値が，自装置のコンフィグレーション値より小さいとき，通知された restart-time の値を使用して監視を行います。

レシーブルータがリスタートルータの再起動前に学習した経路情報を保持しておく時間の上限は BGP4 コンフィグレーションの stale-routes-retain-time サブコマンドで指定します (「図 13-25　グレースフル・リスタートのシーケンス」の (d))。

各パラメータを設定する場合は，一般に次のようにしてください。

- stale-routes-retain-time はリスタートルータの options graceful-restart time-limit より大きい値を設定
  options graceful-restart time-limit は，リスタートルータが経路配布を開始する時間の上限となるので，経路配布が最も遅い場合は，time-limit の経過後にレシーブルータへ経路配布を開始します。レシーブルータで，経路学習およびフォワーディングテーブルの更新後に，古い経路情報が削除されるようにするため，stale-routes-retain-time の指定は，リスタートルータの options graceful-restart time-limit より 120 秒程度長い時間を設定してください。なお，目安の設定値は，経路数およびリスタートルータの隣接ピア数に依存します。

（c） レシーブルータ機能が失敗するケース

以下に，BGP4 のグレースフル・リスタートが失敗するケースを示します。

- グレースフル・リスタートを開始してから，restart-time の時間が経過しても BGP コネクションが再確立しなかった場合，リスタートルータを経由する通信が停止します。
- レシーブルータ機能を実行中に，自装置がリスタートした場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートしているピア装置が，グレースフル・リスタートの開始前に学習していた経路情報を保持できなかった場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートの開始後に，再確立した BGP コネクション上で，リスタートルータからの経路情報の配布が完了する前に，再び切断した場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートの開始後に，リスタートルータから学習した経路数が学習経路数制限機能による上限値を超え，BGP コネクションが再び切断した場合，リスタートルータを経由する通信が停止します。

(5)　グレースフル・リスタート使用時の注意事項

1. TCP MD5 の併用について
   グレースフル・リスタートをサポートする BGP コネクションが確立しているとき，ピアから新しいコネクションの要求を受けた場合，プロトコルの規定によって，確立中の BGP コネクションを破棄し，新しい BGP コネクションを使用します。この動作によるセキュリティ上の問題を防ぐために TCP MD5 認証を併用してください。
2. IGP へ依存する環境でのグレースフル・リスタートについて
   BGP コネクションにルーティングピアを使用し，ピアアドレス宛ての経路情報を IGP によって交換している場合や，ルート・リフレクションを使用する構成などで，BGP 経路情報の NextHop 属性を IGP 経路によって解決する場合は，当該 IGP についてもグレースフル・リスタートの機能を設定してください。

13.3.12　BGP4 経路の安定化機能

(1)　BGP4 セッション切断抑止

直接接続された BGP4 ピアとのインタフェースダウン時，即時に該当ピアとの BGP4 セッションを切断しないことによって，ピアの状態やインタフェース状態が不安定な場合に該当ピアからの経路の再学習回数，および該当ピアへの経路の再広告回数を軽減することができます。この機能はコンフィグレーションコマンド bgp の no-fast-fallover サブコマンドを指定した場合に適用されます。

外部ピアとの間にこの機能を適用した場合の概要を次の図に示します。

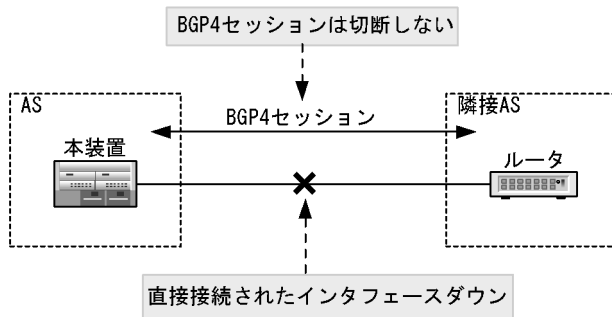
図 13-26　BGP4 コネクション切断抑止機能

インタフェースダウン時の BGP4 セッションの扱いを次の表に示します。

表 13-17　インタフェースダウン時の BGP4 セッションの扱い

ピア接続種別			no-fast-fallover 指定※	
			無し	有り
外部ピア		直接接続	即時に BGP4 セッション切断	確立状態を保持
		multihop	確立状態を保持	確立状態を保持
内部ピア	インターナル	直接接続	即時に BGP4 セッション切断	確立状態を保持
		multihop	確立状態を保持	確立状態を保持
	ルーティング		確立状態を保持	確立状態を保持

注※　インタフェースダウンによってホールドタイムアウトが発生した場合，no-fast-fallover の有無にかかわらず，

BGP4 セッションは切断されます。

(2) BGP4 経路の状態変更遅延

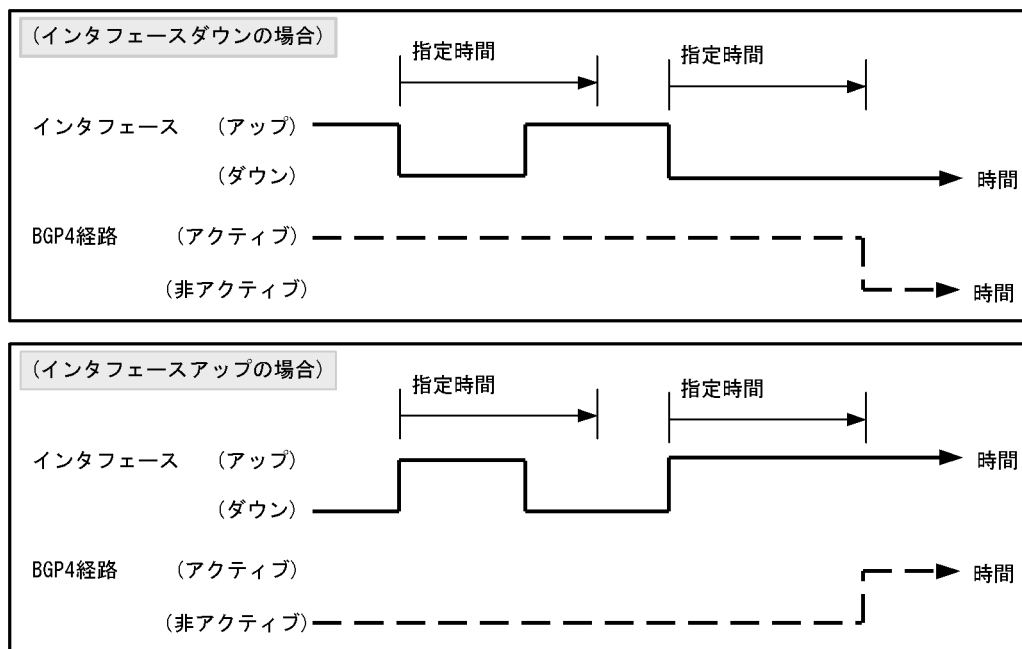
直接接続された BGP4 ピアとのインタフェースダウン，または BGP4 経路のネクストホップ解決に使用している IGP 経路が削除されたことによって，BGP4 経路宛の通信が不可能になった場合も指定時間，該当 BGP4 経路のアクティブ状態を保持します。

また，逆に直接接続された BGP4 ピアとのインタフェースアップ，または BGP4 経路のネクストホップ解決に使用している IGP 経路が復旧後も指定時間，該当 BGP4 経路の非アクティブ状態を保持します。

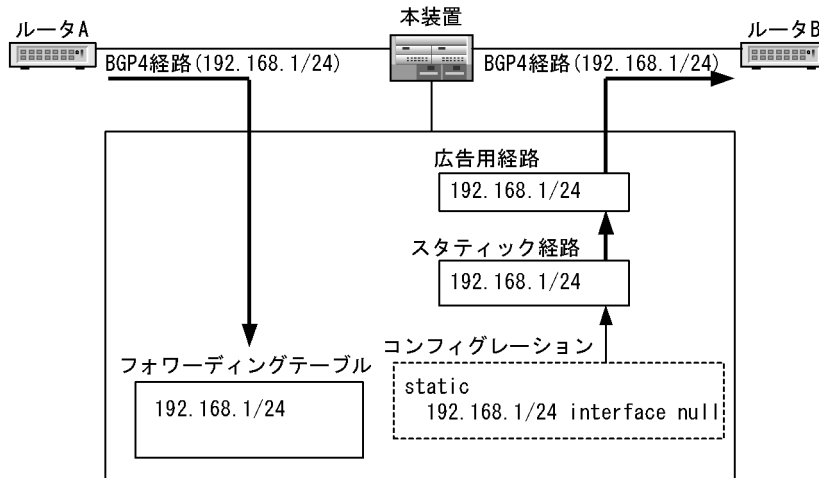
この機能によってインタフェース状態が不安定な場合や，IGP 経路状態が不安定な場合の BGP4 経路のフラップを軽減することができます。

上記指定時間はコンフィグレーションコマンド bgp の route-stability-time サブコマンドで指定します。

インタフェース状態変化による BGP4 経路の扱いを次の図に示します。

図 13-27　インタフェースダウンによる BGP4 経路の扱い

13.3.13　BGP4 広告用経路生成

BGP4 広告用経路生成とは BGP4 経路と同じ宛先の経路情報を自装置内の経路情報から生成して，BGP4 で広告する機能です。パケットのフォワーディング用に実際の BGP4 経路を使用して，他装置広告用には生成した広告用経路を使用することによって，BGP4 経路を宛先とするフォワーディングと安定した経路広告が可能となります。この機能の使用例を次の図に示します。

図 13-28　広告用経路生成と広告

この図ではルータ A から受信した BGP4 経路をフォワーディングテーブルに設定して，該当経路と同じ宛先のスタティック経路から生成された広告用経路をルータ B に広告するように設定しています。

このように設定することで，フォワーディングには BGP4 経路が使用され，かつルータ A から受信する BGP4 経路がフラップした場合でもルータ B への BGP4 経路広告に影響しません。

広告用経路の生成はコンフィグレーションコマンド bgp の network サブコマンドを使用します。また，広告用経路の広告はコンフィグレーションコマンド export，またはコンフィグレーションコマンド route-filter の学習元に proto bgp local を指定します。

13.3.14　BGP4 学習経路数制限

BGP4 学習経路数制限とは，ピアから学習する BGP4 経路の数を制限し，大量の BGP4 経路学習による本装置のメモリ不足や，特定ピアからの大量経路学習によってほかのピアから経路を学習できなくなることを回避するための機能です。この機能はコンフィグレーションコマンド bgp4 の maximum-prefix サブコマンドを指定した場合に適用されます。

この機能を適用すると，ピアから学習した BGP4 経路の数が設定した閾値を超えた場合，警告の運用メッセージを出力します。さらに，上限値を超えた場合は，警告の運用メッセージを出力した後でピアを切断します。この機能によるピア切断後は，設定した期間の経過，または運用コマンド clear ip bgp でピアを再び接続します。また，学習経路数が上限値を超えても，警告の運用メッセージを出力するだけでピアを切断しない設定もできます。

13.3.15　BGP4 使用時の注意事項

BGP4 を使用したネットワークを構成する場合には次の制限事項に留意してください。

(1) BGP4 の制限事項

本装置は RFC1771(BGP バージョン 4 仕様)，RFC2796(ルート・リフレクション仕様)，RFC1997(コミュニティ仕様)，RFC1965(コンフィデレーション仕様)，RFC2842(サポート機能の広告仕様)，RFC2918(ルート・リフレッシュ仕様)に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。なお，本装置は BGP バージョン 4 だけをサポートしています。

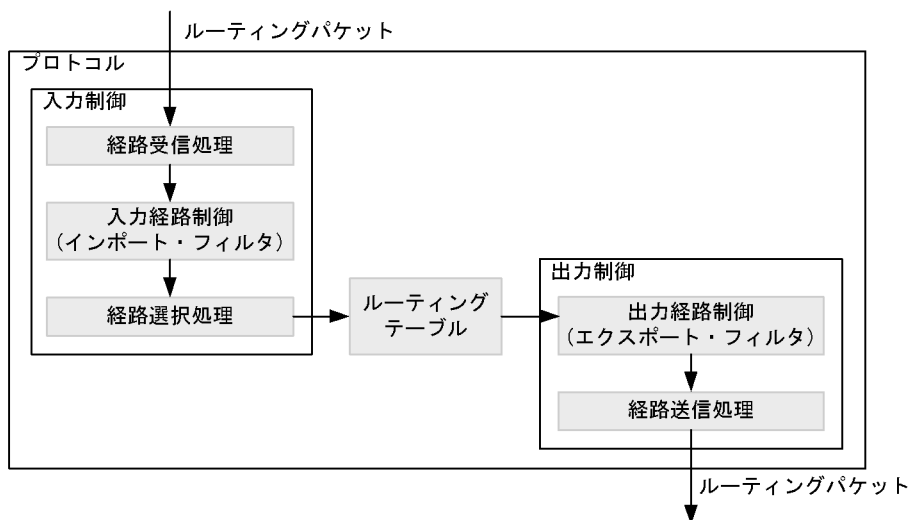
表 13-18　RFC との差分 (RFC1771)

RFC 番号	RFC		本装置
RFC1771	メッセージヘッダ形式	メッセージタイプが OPEN メッセージで認証を持つ場合，Marker の値は認証メカニズムで規定される計算によって予測できます。	認証機能はサポートしていません。
	パス属性：NEXT_HOP	BGP スピーカが，同一 AS 内の BGP スピーカへ経路を広告するとき，広告するスピーカは，その経路に関する NEXT_HOP 属性を修正すべきでありません。	同一 AS 内の BGP スピーカへ経路を広告するとき，NEXT_HOP 属性にその BGP スピーカとのピアリングに使用している自側の IP アドレスを設定します。
	パス属性：ATOMIC_AGGREGATE	BGP スピーカで，そのピアの一つから重複経路のセットが与えられ，より個別の (specific) 経路を選択しないで，より個別ではない経路を選択する場合，ローカルシステムはそのほかの BGP スピーカへ経路を伝えるときに経路に ATOMIC_AGGREGATE 属性を付加すべきです。	ピアの一つから重複経路を受信して個別ではない経路だけをインストールします。それをそのほかの BGP スピーカへ伝えるときは経路に ATOMIC_AGGREGATE 属性を付加しません。
	コネクション衝突の発見	Open メッセージを受信したとき，ローカルシステムは OpenConfirm 状態にあるすべてのコネクションを検査しなければなりません。また，プロトコル以外の手段によってピアの BGP 識別子を知り得るなら，OpenSent 状態のコネクションも検査します。	Open メッセージを受信したとき，OpenSent 状態または Connect 状態のすべてのコネクションを検査します。
	バージョンネゴシエーション	BGP スピーカは，それぞれがサポートする最高のバージョンからはじめ，BGP コネクションのオープンを複数回試みることによって，プロトコルのバージョンを取り決められます。	BGP バージョン 4 だけサポートします。
	BGP FSM：IDLE 状態	エラーのために Idle 状態へ遷移したピアについて，続く Start までの間の時間は (Start イベントが自動的に生成されるなら)，指数的に増大するべきです。その最初のタイマ値は 60 秒です。時間はリトライごとに 2 倍にされるべきです。	Idle 状態から start までの間の最初のタイマは 16 ～ 36 秒です。
	BGP FSM：Active 状態	トランスポート・プロトコル・コネクションが成功した場合，ローカルシステムは ConnectRetry タイマをクリアし，初期設定を完了します。その後，そのピアへ OPEN メッセージを送信してその Hold タイマをセットし，状態を OpenSent に変更します。Hold タイマの値は 4 分が提案されています。	Hold タイマはデフォルトで 180 秒 (3 分)，コンフィグレーションで指定されている場合はコンフィグレーションの値を使用します。
	経路広告の頻度	MinRouteAdvertisementInterval は，単一の BGP スピーカからの特定の宛先への経路広告の間隔の最小時間を決めます。このレート制限は宛先ごとに処理されます。しかし，MinRouteAdvertisementInterval の値は，BGP4 ピアごとに設定されます。	MinRouteAdvertisementInterval はサポートしていません。
		MinASOriginationInterval は，広告する BGP スピーカ自身の AS 中の変化を報告するための連続した UPDATE メッセージ広告の間に経過しなければならない最小時間を決めます。	MinASOriginationInterval はサポートしていません。
	ジッタ	ある BGP スピーカによる BGP メッセージの配布がピークを含む可能性を最小にするために，MinASOriginationInterval,Keepalive, MinRouteAdvertisementInterval に関係したタイマにジッタを適用すべきです。	ジッタを適用していません。

RFC 番号	RFC		本装置
	BGP タイマ	ConnectRetry タイマの提案されている値は 120 秒です。	ConnectRetry 回数によって変化する可変値（16 ～ 148 秒）になります。
		Hold Time の提案されている値は 90 秒です。	デフォルトの Hold Time は 180 秒になります。コンフィグレーションに Hold Time が設定されている場合は，その値を使用します。
		KeepAlive タイマの提案されている値は 30 秒です。	Hold Time の 1/3 になります。
		BGP の実装は，これらのタイマがコンフィグレーションで定義できなければなりません。	Hold Time だけがコンフィグレーションで定義できます。
RFC1965	メンバー AS 間ピアに経路情報を広告する場合，AS_PATH 属性にタイプ AS_CONFED_SEQUENCE で自メンバー AS 番号を追加します。		AS_PATH 属性にタイプ AS_CONFED_SET で自メンバー AS 番号を追加します。

13.4　経路フィルタリング (BGP4)

経路フィルタリングには，入力経路を制御するインポート・フィルタと出力経路を制御するエキスポート・フィルタがあります。インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。エキスポート・フィルタは同一ルーティングプロトコル，またはルータ上で同時に動作している異なるプロトコルで学習した経路を広告するかどうかを制御します。フィルタリングの概念を次の図に示します。

図 13-29　フィルタリングの概念

13.4.1　インポート・フィルタ (BGP4)

インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。インポート・フィルタを指定していない場合は，すべての経路情報を取り込みます。

(1) プリファレンス値

取り込む経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，そのプロトコルのデフォルトのプリファレンス値になります。

同一宛先アドレスの経路情報が複数存在する場合，プリファレンス値によって優先度の高い経路情報が有効となります。プリファレンス値の詳細は，「12.3.3　スタティックルーティングとダイナミックルーティング (RIP/OSPF) の同時動作　(1) プリファレンス値」を参照ください。

(2) フィルタリング条件

取り込む経路情報はフィルタリング条件で指定できます。指定できるインポート・フィルタのフィルタリング条件を次に示します。

- 送信元ピアアドレス
- 送信元 AS 番号
- 送信元ポリシーグループ番号
- 経路情報の AS_PATH 属性
- 経路情報の ORIGIN 属性

- 経路情報の Community 属性
- 経路情報の宛先ネットワーク

また，取り込まれた経路情報はフィルタリング条件ごとにその経路情報の BGP 属性を変更できます。変更できる BGP 属性を次に示します。

- LOCAL_PREF 属性
- AS_PATH 属性 (追加 AS 数を指定する)
- ORIGIN 属性
- MED 属性
- Community 属性 (削除または追加 Community を指定する)

(3) 拡張正規表現

フィルタリング条件である AS_PATH 属性や COMMUNITY 属性は，拡張正規表現 (Extended Regular Expression) によって，1 文字単位に複数の意味を持つ文字列で指定できます。

拡張正規表現には，数字，小文字アルファベット，大文字アルファベット，記号 (ただし，ダブルクォーテーション (") は除く) などの通常文字と，次に示す特殊文字が使用可能です。

- .　：空白を含むすべての単一文字を意味します。
- *　：文字や文字集合の 0 回以上の繰り返しを意味します。
- +　：文字や文字集合の 1 回以上の繰り返しを意味します。
- ?　：文字や文字集合の 0 回もしくは 1 回を意味します（コマンド入力時には［Ctrl］+［V］を入力後［?］を入力してください)。
- ^　：文字列の先頭を意味します。文字範囲を示す [ ] の中の先頭に置いた場合，パターンの否定を意味します。
- $　：文字列の末尾を意味します。
- _　：文字列の先頭，文字列の末尾，「 」(空白)，「_」，「,」，「(」(通常文字)，「)」(通常文字)，「{」，「}」，「<」，「>」のどれかを意味します。
- [ ]　：[ ] 内の文字範囲のうち単一文字を意味します。[ ] 内で特殊文字を使用した場合には通常文字として扱います (特殊文字としても意味は持ちません)。
- -　：[ ] の中で範囲のうち開始と終了を示すために使用します。- の前の文字は - の後の文字よりも文字コードが小さくなるように指定してください。文字コードについては「コンフィグレーションコマンドレファレンス Vol.1　パラメータに指定できる値」を参照してください。
  例：[6-8] は 678 のどれか 1 文字を意味します。[^6-8] は 678 以外のいずれか 1 文字を意味します。
- ( )　：複数文字の集合を意味します。最大で 9 集合までネスト可能です。
- |　：OR 条件を意味します。
- ¥　：上記の特殊文字の前に置いた場合，通常文字として扱います。

コンフィグレーションコマンドや運用コマンドで拡張正規表現を指定する際には，拡張正規表現の前後をダブルクォーテーション (") で括って指定してください。

例：
```
# show ip bgp aspath-regexp "^$"
(config)# attribute-list attribute-filter 1 aspath-regexp "_100_"
```

拡張正規表現で使用する文字同士の結合の優先順位は次の表に示す様になります。

表 13-19　拡張正規表現使用文字の結合の優先順位

優先順位	文字
高	( )

優先順位	文字
↑	*，+，?
↓	通常文字，.，[ ]，^，$
低	|

AS_PATH 属性は，パスタイプごとに次の様に表現します。

AS_SEQ： <AS 番号 > …

AS_SET：{ <AS 番号 > … }

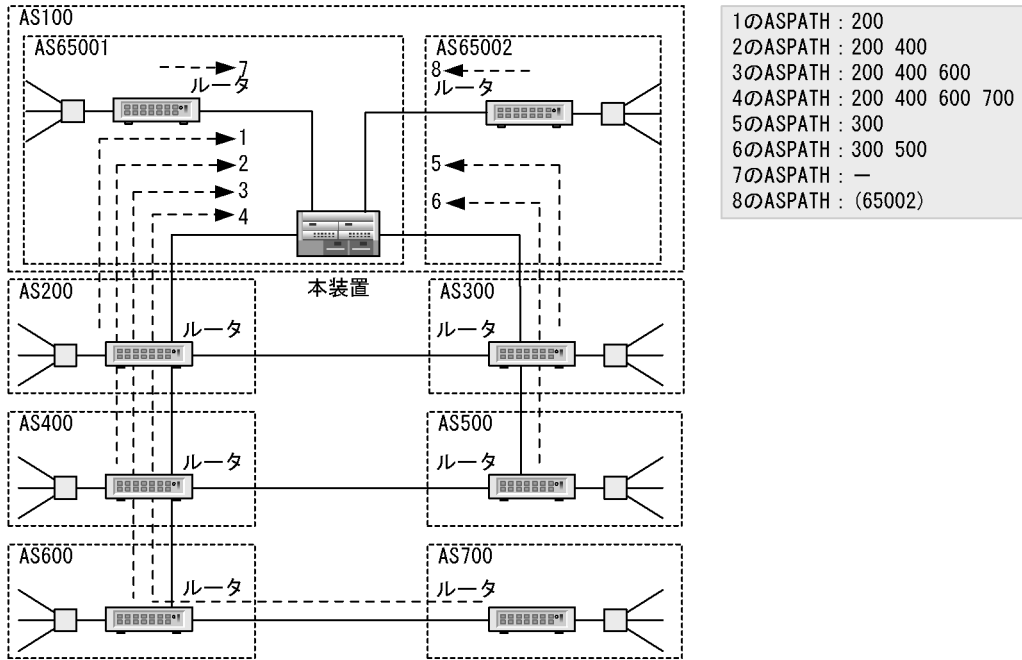
AS_CONFED_SET：(<AS 番号 > …)

注　<AS 番号 > は 10 進数で表します。

AS_CONFED_SET を表す ( ) は特殊文字として使用されていますので，AS_CONFED_SET の意味で使用する際には，¥ を付けることに注意してください。

例：¥(65001 65002¥)

拡張正規表現を用いた AS パスの指定例を次の図に示します。

図 13-30　拡張正規表現を用いた AS パス指定例

1のASPATH：200
2のASPATH：200 400
3のASPATH：200 400 600
4のASPATH：200 400 600 700
5のASPATH：300
6のASPATH：300 500
7のASPATH：－
8のASPATH：(65002)

項目	拡張正規表現指定例
隣接するAS200内に存在するネットワークへの経路（1）	^200$
隣接するAS200から通知された経路（1，2，3，4）	^200_
隣接するAS200から通知された経路であるが，宛先ネットワークはAS200に属さないネットワークである経路（2，3，4）	^200_.+
隣接するAS内に属するネットワークへの経路（1，5）	^[0-9]+$
隣接するAS内に属さないネットワークへの経路（2，3，4，6）	^[0-9]+_.+
自ASから二つまたは三つ離れたASに属するネットワークへの経路（2，3，6）	^[0-9]+_[0-9]+_([0-9]+)?$
AS600を経由する経路（3，4）	_600_
AS_PATH属性を持たない経路（7）	^$
パスタイプAS_CONFED_SETを持つ経路（8）	_¥(.*¥)_
プライベートAS(AS番号64512～65535)を持つ経路（8）	_(6451[2-9]|645[2-9][0-9]|64[6-9][0-9][0-9]|65[0-9][0-9][0-9])_

Community 属性は，次の様に表現します。

<AS 番号 >:< 値 >

no-export　：0xFFFFFF01(16 進数) を示します。

no-advertise　：0xFFFFFF02(16 進数) を示します。

no-export-sub　：0xFFFFFF03(16 進数) を示します。

注　<AS 番号 > や < 値 > は 10 進数で表します。

拡張正規表現を用いた Community の指定例を次の図に示します。

図 13-31 拡張正規表現を用いた Community 指定例

```
1のCOMMUNITY：200:40
2のCOMMUNITY：200:60
3のCOMMUNITY：600:40
4のCOMMUNITY：600:60
5のCOMMUNITY：100:1 200:2 300:3
6のCOMMUNITY：－
7のCOMMUNITY：no-export
8のCOMMUNITY：no-advertise
9のCOMMUNITY：no-export-sub
```

項目	拡張正規表現指定例
COMMUNITY属性を持っている経路(1, 2, 3, 4, 5, 7, 8, 9)	.+
COMMUNITY属性を持っていない経路（6）	^$
COMMUNITY属性 no-exportだけを持っている経路(7)	^no-export$
COMMUNITY属性 no-export, no-advertise, no-export-sub のいずれかを持っている経路（7, 8, 9）	no-
COMMUNITY属性のAS番号が200(10進数)を持っている経路（1, 2, 5）	_200:[0-9]+_
COMMUNITY属性の値が40(10進数)を持っている経路（1, 3）	_[0-9]+:40_
COMMUNITY属性200:60だけを持っている経路（2）	^200:60$

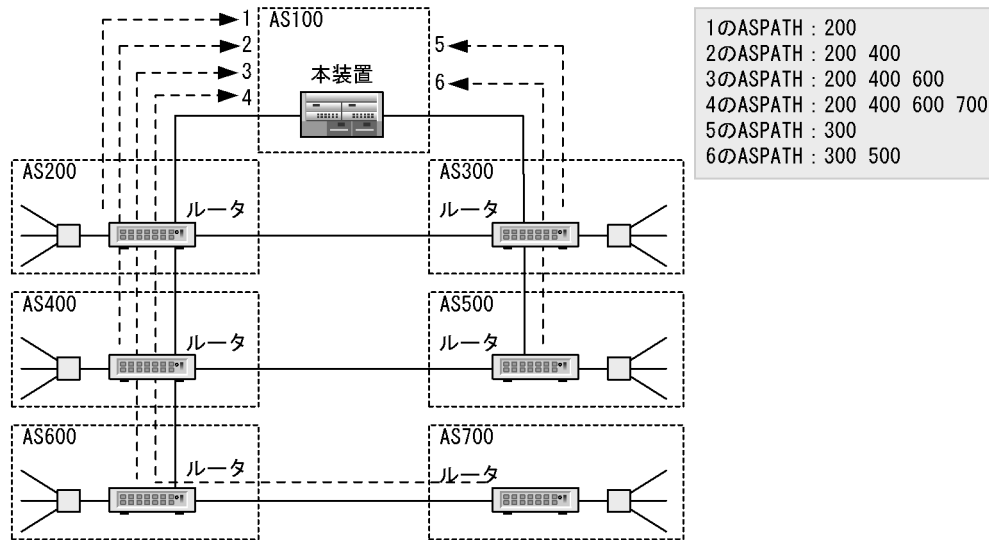
(4) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) によって複数の AS_PATH に一致するような表現で指定できます。AS パス正規表現は次の形式で指定します。

```
<Aspath> := {<Aspath_Term>...|^$}
<Aspath_Term> := <Aspath_Symbol>[{ {m,n} | {m} | {m,} | * | + | ? }]
<Aspath_Symbol> := { <As> | .}
```

- ^$ ：空の AS パスを意味します。
- {m,n}：Aspath_Symbol を m 回から n 回，繰り返すことを意味します。
  (m,n の設定範囲：0 ～ 255)
- {m} ：Aspath_Symbol を m 回，繰り返すことを意味します。
  (m の設定範囲：0 ～ 255)
- {m,} ：Aspath_Symbol を m 回以上，繰り返すことを意味します。
  (m の設定範囲：0 ～ 255)
- * ：Aspath_Symbol を 0 回以上，繰り返すことを意味します。
- + ：Aspath_Symbol を 1 回以上，繰り返すことを意味します。
- ? ：Aspath_Symbol を 0 回または 1 回，繰り返すことを意味します。
- <As>：指定した AS 番号を意味します。
- . ：任意の AS 番号を意味します。

AS パス正規表現の例を次の図に示します。

図 13-32　AS パス正規表現の例

項目	ASパス正規表現
隣接するAS200内に存在するネットワークへの経路（1）	200
隣接するAS200から通知された経路（1，2，3，4）	200.*
隣接するAS200から通知された経路であるが，宛先ネットワークはAS200に属さないネットワークである経路（2，3，4）	200.+
隣接するAS内に属するネットワークへの経路（1，5）	.{1}
隣接するAS内に属さないネットワークへの経路（2，3，4，6）	.{2,}
自ASから二つまたは三つ離れたASに属するネットワークへの経路（2，3，6）	.{2,3}
AS600を経由する経路（3，4）	.* 600.*

（5）MED 属性値

インポート・フィルタと次に示すパラメータの組み合わせによって，学習した BGP4 経路情報の MED 属性値を変更できます。

- コンフィグレーションコマンド attribute-list の med サブコマンド
- コンフィグレーションコマンド route-filter の med パラメータ

med サブコマンド（パラメータ）の指定値は，数値指定とオフセット指定があります。

インポート・フィルタと組み合わせた med サブコマンド（パラメータ）でオフセット指定（±指定）した場合に，学習経路情報に設定される MED 属性値を次の表に示します。

表 13-20　オフセット指定した場合に取り込む経路情報の MED 属性値

学習元プロトコル	MED 属性値
BGP4	• 経路情報に MED 属性値が含まれている場合，経路情報の MED 属性値にオフセット値を±した値を使用します。 • 経路情報に MED 属性値が含まれていない場合，0 を基準にオフセット値を±した値を使用します。

注　オフセット値を±した結果がマイナスになった場合は 0 に，4294967295 を超えた場合は 4294967295 に値が補正されます。

13.4.2　エキスポート・フィルタ (BGP4)

エキスポート機能はルータ上で同時に動作しているルーティングプロトコル間で経路情報を再配布します。つまり，学習元プロトコルで学習した経路情報を，配布先プロトコルを使用してそのほかのシステム(ルータ)に広告します。

(1) フィルタリング条件

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件(送出先)と学習元プロトコルのフィルタリング条件(送出経路情報)によって，特定の宛先に特定の経路情報を送出できます。また，配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値になります。

指定できるフィルタリング条件を配布先プロトコルと学習元プロトコルに分け「表 13-21　配布先プロトコルのフィルタリング条件」と「表 13-22　学習元プロトコルのフィルタリング条件」に示します。なお，配布先プロトコルが，RIP または OSPFASE の場合は，「12.6.2　エキスポート・フィルタ (RIP/OSPF)」を参照してください。

表 13-21　配布先プロトコルのフィルタリング条件

フィルタリング条件 (送出先)	付加情報
• 送信先ピアアドレス • 送信先ポリシーグループ番号 • 送信先 AS 番号	• LOCAL_PREF 属性 • 追加 AS パス長 • ORIGIN 属性 • MED 属性 • Community 属性

表 13-22　学習元プロトコルのフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIP	• 受信インタフェース • 送信元ゲートウェイ • 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIP で学習された経路情報
OSPF	• OSPF ドメイン番号 • 経路情報の宛先ネットワーク	OSPF で学習された経路情報
OSPFASE	• OSPF ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPF の AS 外経路情報
BGP4	• 送信元ピアアドレス • 送信元 AS 番号 • 送信元ポリシーグループ番号 • 経路情報の AS_PATH 属性 • 経路情報の ORIGIN 属性 • 経路情報の Community 属性 • 経路情報の宛先ネットワーク	BGP4 で学習された経路情報
IS-IS	• 学習元レベル • 経路情報の経路種別 • 経路情報のメトリック種別 • 経路情報の宛先ネットワーク	IS-IS で学習された経路
DIRECT	• インタフェース • 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 送出元インタフェース • 経路情報の宛先ネットワーク	スタティックの経路情報

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
DEFAULT	• 経路情報の宛先ネットワーク	BGP4 の DEFAULT 経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

(2) 再配布する経路情報の MED 属性値

再配布する経路情報の MED 属性値を指定するには，次に示すパラメータを使用します。

- エキスポート・フィルタと組み合わせた，コンフィグレーションコマンド attribute-list または route-filter の med サブコマンド (パラメータ)
- コンフィグレーションコマンド bgp の defaultmetric サブコマンド

再配布する経路情報の MED 属性値を「表 13-23　再配布する経路情報の MED 属性値」に示します。また，エキスポート・フィルタと組み合わせた med サブコマンド (パラメータ) でオフセット指定 (±指定) した場合，再配布する経路情報の MED 属性値を「表 13-24　オフセット指定した場合に再配布する経路情報の MED 属性値」に示します。

表 13-23　再配布する経路情報の MED 属性値

med 指定	学習元プロトコル	メトリック値
あり	全プロトコル共通	エキスポート・フィルタで指定した MED 属性値を使用します。
なし	BGP4	外部ピアから学習した経路情報を内部ピアに広告する場合，経路情報の MED 属性値を引き継ぎます。そのほかの場合，コンフィグレーションコマンド bgp の defaultmetric サブコマンドで指定した値を使用します。defaultmetric サブコマンドの指定がない場合は MED 属性値を設定しません。
	その他	コンフィグレーションコマンド bgp の defaultmetric サブコマンドで指定した値を使用します。defaultmetric サブコマンドの指定がない場合は MED 属性値を設定しません。

表 13-24　オフセット指定した場合に再配布する経路情報の MED 属性値

学習元プロトコル	MED 属性値
全プロトコル共通	「表 13-23　再配布する経路情報の MED 属性値」に示している再配布時に使用する経路情報の MED 属性値に，オフセット値を±した値を使用します。ただし，経路情報に MED 属性値が設定されていない場合は，0 を基準にオフセット値を±した値を使用します。

注　オフセット値を±した結果がマイナスになった場合は 0 に，4294967295 を超えた場合は 4294967295 に値が補正されます。

(3) 拡張正規表現

フィルタリング条件である AS_PATH 属性や COMMUNITY 属性は，拡張正規表現 (Extended Regular Expression) によって 1 文字単位に指定できます。拡張正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)　(3) 拡張正規表現」を参照してください。

(4) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) によって複数の AS_PATH に一致するような表現で指定できます。AS パス正規表現の指定形式は「13.4.1　イン

ポート・フィルタ (BGP4) （4）AS パス正規表現」を参照してください。

（5） エキスポート設定時の注意事項

BGP4 は同一のルーティングプロトコルで学習した経路情報であっても，エキスポートを定義しないと経路情報を広告しないので注意してください。

13.5 経路集約 (BGP4)

経路集約は一つまたは複数の経路情報から，該当する経路情報を包含するネットワークマスクのより短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含する一つの経路情報を生成し，隣接ルータなどに集約経路を通知して，ネットワーク上の経路情報の数を少なくする方法です。例えば，172.16.178.0/24 の経路情報や 172.16.179.0/24 の経路情報を学習した場合に，172.16.0.0/16 の集約された経路情報を生成するなどです。

経路集約の指定は AGGREGATE(経路集約) コマンドで明示的に指定する必要があります。集約元の経路情報はフィルタリング条件によって特定できます。集約元経路情報のフィルタリング条件を次の表に示します。

表 13-25　集約元経路情報のフィルタリング条件

集約元プロトコル	フィルタリング条件 (集約元経路情報)	備考
RIP	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIP で学習された経路情報
OSPF	• 経路情報の宛先ネットワーク	OSPF で学習された経路情報
OSPFASE	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPF の AS 外経路情報
BGP4	• 送信元 AS 番号 • 経路情報の AS_PATH 属性 • 経路情報の ORIGIN 属性 • 経路情報の宛先ネットワーク	BGP4 で学習された経路情報
IS-IS	• 学習元レベル • 経路情報の経路種別 • 経路情報のメトリック種別 • 経路情報の宛先ネットワーク	IS-IS で学習された経路
DIRECT	• 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 経路情報の宛先ネットワーク	スタティックの経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

また，集約元経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，集約経路のデフォルトのプリファレンス値 (130) が使用されます。なお，集約元の経路情報が学習されていない場合には集約経路情報は生成されません。

(1) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) によって，複数の ASPath に一致する表現で指定できます。

AS パス正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4) (4) AS パス正規表現」を参照してください。

(2) 集約元経路の広告抑止

集約元経路の広告抑止の詳細は，「12.7　経路集約 (RIP/OSPF) (1) 集約元経路の広告抑止」を参照してください。

(3) 集約経路の転送方法

集約経路によるパケット転送方法の詳細は，「12.7　経路集約 (RIP/OSPF)　(2) 集約経路の転送方法」を参照してください。

14 IS-IS【OP-ISIS】

この章では，ルーティングプロトコル IS-IS について説明します。

14.1 IS-IS 概説

IS-IS は，ルータ間の接続の状態から構成されるトポロジに基づき最短経路を計算するリンクステートプロトコルです。本装置では，IS-IS プロトコル機能の中で，IPv4 ルーティング機能と IPv6 ルーティング機能をサポートします。

IS-IS は通常，一つの AS 内部でのルーティングに使用します。IS-IS が動作しているルータでは，そのルータの IS-IS ルーティングについての経路情報を，ほかの IS-IS ルータと共有します。各ルータは，ネットワーク上の IS-IS ルータより収集した経路情報に基づき，最短経路を計算します。

(1) RIP との比較

IS-IS は，同じく AS 内ルーティングプロトコルである RIP と比較して，以下の特徴があります。

- 経路情報のトラフィックの削減
  IS-IS では，ルータ間の接続や，ルータの広告経路の状態が変化したときだけ，変更情報をほかのルータへ通知します。このため，RIP のような定期的にすべての経路情報を通知するルーティングプロトコルと比較して，ルーティングプロトコルが占有するトラフィックが少なくなります。なお，IS-IS では，デフォルトでは 15 分周期で自ルータの接続状態だけをほかのルータに通知します。
- ルーティングループの抑止
  IS-IS では，すべてのルータで保持している経路情報が同じです。このため，各ルータの経路情報の不一致によるルーティングループを防ぐことができます。
- 大規模なネットワーク運用
  IS-IS では，経路選択に使用するメトリック値の上限は，1023 または 4261412864 です（この上限値は選択可能です）。メトリック値の上限が 16 である RIP と比較して，よりホップ数の大きなネットワークにも適用できます。また，インタフェースや IS-IS へ広告する経路のメトリックを加減することによって，RIP よりも柔軟にルーティングすることができます。
- 可変長サブネット
  IS-IS では，経路情報にネットワークマスクを含んでいるので，CIDR 経路を自由に扱えます。一方，RIP-1 では，ナチュラルマスク（宛先 IP アドレスのクラスに従ったネットワークマスク）以外の経路情報の広告に制限があります。

(2) OSPF との比較

IS-IS は，同じくリンクステートルーティングプロトコルである OSPF・OSPFv3 と比較して，以下の特徴があります。

- プロトコル体系の違い
  IS-IS は，元来 OSI プロトコル体系のルーティングプロトコルです。このため，IS-IS の情報交換には，OSI パケットを使用します。
  OSPF・OSPFv3 は，それぞれ IPv4・IPv6 プロトコル体系のルーティングプロトコルなので，それぞれ IPv4 パケット・IPv6 パケットを使用します。
- IPv4 ルーティング・IPv6 ルーティングを同時に扱う
  IS-IS では，一つのルーティングプロトコルで IPv4 と IPv6 を同時に扱います。一方，OSPF は IPv4 をルーティングするプロトコル，OSPFv3 は IPv6 をルーティングするプロトコルです。
  同時に扱うことの長所は，ルーティングプロトコルが一つで済むため，ネットワークの構築・維持が簡潔になることです。
  同時に扱うことの短所は，IPv4 と IPv6 でルーティングプロトコルが同一であるため，IPv4 と IPv6 の間で異なる最短経路の判断方法を適用できないことです。また，IS-IS ネットワーク上の全ルータ・全

回線が IPv4・IPv6 をともにサポートしない限り，IS-IS ネットワークで IPv4・IPv6 を同時にルーティングすることはできません。

- エリア分割方式
  IS-IS の方が，OSPF よりも自由にエリア分割をすることができます。これは，エリア分割方式が異なるためです。
  IS-IS では，エリア分割時に，分割した各エリアのネットワークをレベル 1，エリア間接続に使用する回線とルータからなるネットワークをレベル 2 といいます。各エリアのネットワークは，レベル 2 ネットワークを通して接続されます。レベル 2 ネットワークを構成するルータは，あらかじめネットワーク構築時に指定しておきます。レベル 2 ルータ間の回線は，自動的にレベル 2 回線になります。レベル 2 回線が，同時にあるエリアのレベル 1 回線であってもかまいません。
  OSPF では，エリア分割時に，中心となるエリアをあらかじめ作成しておきます。このエリアをバックボーンといいます。バックボーン以外のエリアは，バックボーンエリアと，エリア境界ルータを通じて接続している必要があります。どの回線も，所属できるエリアは一つだけです。バックボーン上の回線が，同時にほかのエリアの回線になることはありません。
  一般には，IS-IS のエリア分割の方が柔軟である一方，レベル 2 ネットワークが大きくなり，レベル分割の利点が小さくなる傾向があります。

(3) サポート仕様

IS-IS ルーティング機能のサポート仕様を次の表に示します。

表 14-1　IS-IS サポート機能

IS-IS 機能	仕様
IPv4 ルーティング (RFC 1195 準拠)	○
IPv6 ルーティング (“draft-ietf-isis-ipv6-05.txt” Internet Draft 準拠)	○
OSI ルーティング	×
IS-IS プロトコルパケット交換サポートインタフェース	「表 14-2　IS-IS サポート回線種別とその通信方式」を参照
イコールコストマルチパス	○
エリア分割	○
ドメインワイド拡張 (RFC 2966 準拠)	○
IPv4 ルーティング メトリック拡張 (“draft-ietf-isis-traffic-04.txt” Internet Draft 準拠)	○
トラフィック・エンジニアリング対応	×
ホスト名交換拡張 (RFC2763 準拠)	○
暗号化認証 (“draft-ietf-isis-hmac-03.txt” Internet Draft 準拠)	○
再配布経路およびレベル間広告経路の集約広告	○
グレースフル・リスタート (RFC3847 準拠)	○※

(凡例) ○：取り扱う　　×：取り扱わない
注※　SB-5400S ではヘルパー機能だけサポートします。

回線種別および通信方式に基づき，IS-IS プロトコルパケット交換のサポート・未サポートを次の表に示します。仕様に記述の IS-IS インタフェース種別については，「14.2.1　経路情報広告の基礎　(4) IS-IS

インタフェース」を参照ください。

表 14-2　IS-IS サポート回線種別とその通信方式

<table>
<tr><th>回線種別</th><th>インタフェース</th><th>通信方式</th><th>仕様</th></tr>
<tr><td rowspan="4">LAN</td><td rowspan="3">• イーサネット
(RM イーサネット（SB-5400S ではリモートマネージメントポート）を除く)</td><td>Ethernet V2</td><td rowspan="2">○
ブロードキャスト型インタフェース</td></tr>
<tr><td>802.3</td></tr>
<tr><td>VLAN</td><td>○
ブロードキャスト型インタフェース</td></tr>
<tr><td>• RM イーサネット（SB-5400S ではリモートマネージメントポート）</td><td>Ethernet V2</td><td>×</td></tr>
<tr><td>WAN</td><td>POS</td><td>PPP
(ポイント - ポイント型)</td><td>○
ポイント - ポイント型インタフェース</td></tr>
</table>

(凡例)　○：取り扱う　　×：取り扱わない

（4） IS-IS 使用上の注意

1. IS-IS を使用する場合，以下の注意事項を参照してください。
   「14.2.1　経路情報広告の基礎　(2) サポートプロトコル体系　【注意事項】」
   「14.2.1　経路情報広告の基礎　(4) IS-IS インタフェース　【注意事項】」
2. IS-IS でエリア分割を使用する場合，以下の注意事項を参照してください。
   「14.2.2　エリア分割とレベル　(1) レベルとエリア　【注意事項】」
3. IS-IS で認証を使用する場合，以下の注意事項を参照してください。
   「14.2.5　認証 (IS-IS)　(1) 隣接ルータの認証　【注意事項】」
   「14.2.5　認証 (IS-IS)　(2) LSP の認証　【注意事項】」
4. IS-IS でグレースフル・リスタート機能を使用する場合，以下の注意事項を参照してください。
   「14.2.8　グレースフル・リスタート　(2) リスタート機能【SB-7800S】 (d) 注意事項」
   「14.2.8　グレースフル・リスタート　(3) ヘルパー機能　(c) 注意事項」

14.2　IS-IS

この節では IS-IS プロトコルと，エキスポート機能による IS-IS への経路再配布について説明します。

14.2.1　経路情報広告の基礎

（1） ルーティングドメイン (または単にドメイン)

一つのルーティングプロトコルにより経路を管理しているネットワークの範囲のことを，ルーティングドメイン，または単にドメインと呼びます。

IS-IS プロトコルで相互接続しており，IS-IS を使用してルーティングをしている部分のネットワークを，IS-IS ルーティングドメイン，または単に IS-IS ドメインと呼びます。

（2） サポートプロトコル体系

IS-IS では，複数のプロトコル体系のルーティングを同時にサポートすることができます。

本装置では，IPv4 および IPv6 のルーティングをサポートしています。本装置は，デフォルトでは，IPv4 経路だけをルーティングします。

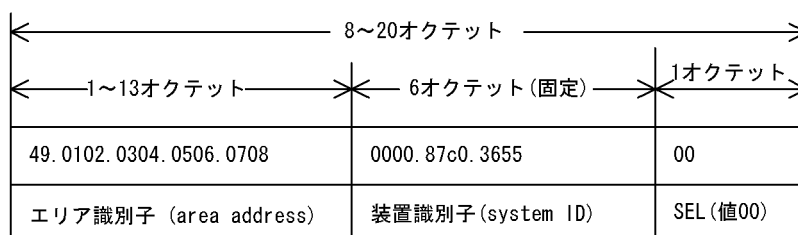
ルーティングするプロトコルは，全ルータで統一してください。

【注意事項】

IS-IS で IPv4 ルーティングを行う場合，IS-IS ドメイン上の全ルータを，IS-IS で IPv4 ルーティングをするよう設定する必要があります。また，隣接ルータと接続する全インタフェースを，IPv4 パケットを送受信できるよう設定する必要があります。
同様に，IS-IS で IPv6 ルーティングを行う場合，IS-IS ドメイン上の全ルータを，IS-IS で IPv6 ルーティングをするよう設定する必要があります。また，隣接ルータと接続する全インタフェースを，IPv6 パケットを送受信できるよう設定する必要があります。
また，IPv4 と IPv6 の両方をルーティングする場合も，上記設定が必要です。
上記条件が満たされない場合，隣接ルータ間で IS-IS プロトコルが接続しないことがあります。また，IS-IS が求めた経路が，該当プロトコル体系の通信機能がないルータ・インタフェースおよび回線を使用する経路となることがあります。

（3） NET

IS-IS では，IS-IS ルータに NET (Network Entity Title) を定義します。NET は，エリア識別子 (area address)，装置識別子 (system ID)，SEL (ルータでは必ず 0 を使用する) の三つのフィールドから成り立っています。NET のフォーマットを次の図に示します。例では，NET として，値 49.0102.0304.0506.0708.0000.87c0.3655.00 を使用しています。

図 14-1　NET のフォーマット

- エリア識別子
  エリア識別子は，IS-IS ネットワーク上でのエリアを区別するための数値です。1 オクテット以上 13 オクテット以下の 16 進数として表記します。エリア識別子が同じルータは，同じエリアに所属しています。2 台のルータ間でエリア識別子が異なる場合，この 2 台のルータのエリアは異なります。エリア識別子の長さが異なる場合，エリアは異なるものとして扱います。
  エリア識別子には，先頭 1 オクテットが 49（16 進）で始まるアドレスを使用することを推奨します。これは，NET は本来 OSI プロトコル体系のアドレスであること，および OSI の規定によると，独自に構成した OSI ネットワーク上では，アドレスの先頭 1 オクテットが 49（16 進）でなければならないとされていることに由来します。
  エリア分割を行わない場合，全ルータのエリア識別子を同じに設定してください。エリア識別子が複数存在すると，IS-IS ではエリア分割をしているものとして動作します。
  エリア分割を行わない場合，全ルータをレベル 1-2 ルータとして設定してください。レベル 1 で動作しないルータが含まれている場合，適切ではない経路を選択することがあります。また，レベル 2 で動作しないルータが含まれている場合，IS-IS の外部から導入した経路について，通信ができないルータが発生します。
  エリア分割については，「14.2.2　エリア分割とレベル」をご参照ください。
  「図 14-1　NET のフォーマット」の例では，エリア識別子に 49.0102.0304.0506.0708 を使用しています。
- 装置識別子
  装置識別子は，IS-IS ネットワーク上の各ルータを区別するための数値です。6 オクテットの 16 進数として表記します。
  IS-IS ネットワーク上の複数のルータに，同じ装置識別子を設定しないでください。装置識別子の同じルータが 2 台以上存在する場合，正しい経路を生成しません。
  「図 14-1　NET のフォーマット」の例では，装置識別子に 0000.87c0.3655 を使用しています。
- SEL
  SEL は，OSI プロトコル体系において，トランスポート層の通信セッションを区別するための数値です。1 オクテットの 16 進数として表記します。
  IS-IS では，ネットワーク層のルーティングプロトコルを示す値’00’を使用します。
  「図 14-1　NET のフォーマット」の例でも，SEL の値に 00 を使用しています。

（4） IS-IS インタフェース

IS-IS では，経路情報の交換に IPv4 パケットも IPv6 パケットも使用しません。代わりに，OSI プロトコル体系の OSI パケットを使用します。

IPv4 や IPv6 と OSI とでは，回線上でのパケットカプセル化方式が異なります。このため，同一回線上でも，IPv4・IPv6 の MTU と，OSI の MTU とは異なります。

OSI では，OSI パケットの送受信上，ルータ間を接続する回線や LAN を，三つの種類に分類します。

- broadcast
  回線上にルータやホストを多数接続することができ，かつ一つのパケットを，同時に多数のルータやホストへ送信することができる回線を，broadcast subnetwork に分類します。
  イーサネットなどの LAN が，これに該当します。
- generic topology（未サポート）
  複数の回線から構成されており，各回線が 1 台の対向装置と接続しているネットワークを，generic topology subnetwork に分類します。
  ATM や WAN のポイント - マルチポイント回線が，これに該当します。
- point-to-point

ネットワーク上に回線が一つしかなく，この回線上に対向装置が 1 台だけ存在するネットワークを，point-to-point subnetwork に分類します。
ATM や WAN のポイント - ポイント回線が，これに該当します。

【注意事項】

1. IS-IS インタフェースの，IS-IS パケット送受信上の MTU は，1492 オクテット以下に設定しないでください。MTU が 1492 オクテット以下である IS-IS インタフェースが存在する場合，該当インタフェース上の隣接ルータと正常にパケット交換ができないことがあります。
2. PPP で 2 台の装置を接続した場合，OSI プロトコル体系では point-to-point と認識されます。
上記ネットワークは，IPv4・IPv6 プロトコル体系ではブロードキャストインタフェースとして動作させる場合もありますが，IPv4/IPv6 プロトコル体系での動作方式と，OSI プロトコル体系での回線種別には，関係がありません。
3. IS-IS インタフェースとして使用する Line には，イーサネットのジャンボフレームを設定しないでください。設定した場合，隣接ルータ間で IS-IS プロトコルが接続しないことがあります。

（5） LSP

IS-IS では，ルータの広告情報はすべて LSP (リンクステート PDU) というパケットに納められています。各ルータは，レベルごとに，LSP を 256 個まで生成することができます。LSP の長さは最大 1492 オクテットです。

実際には，LSP ヘッダの 27 オクテット，および LSP のフォーマット形式のオーバヘッドにより，1 ルータのレベルごとの広告情報量は，約 340 キロオクテットになります。

1 台のルータが一つのレベルに広告できる経路数は，IPv4・IPv6 の広告情報量をあわせて，約 340 キロオクテットまでとなります。IPv4 だけの場合はおよそ 30,000 経路，IPv6 だけの場合はおよそ 15,000 経路が上限になります。

広告情報一つ当たりの情報量については，「表 14-6　TLV の種別」をご参照ください。

（6） 広告方式

本装置では，2 種類の IS-IS 広告方式をサポートしています。この広告方式を，それぞれナロウとワイドと呼びます。広告方式や広告経路のプロトコル体系に応じて，広告できる経路属性情報やその値の範囲が異なります。基本的には，次の方針に従って広告方式を選択してください。

- IS-IS ネットワーク内の全ルータで同じ広告方式を選択してください。既存の IS-IS ネットワークに装置を導入する場合は，既存ネットワークの広告方式と合わせて設定してください。
- IS-IS で IPv6 ルーティングを行う場合，ワイドを選択してください。IPv6 経路情報はワイドの広告形式と近いからです。また，装置によってはナロウを選択すると IPv6 経路を扱えません。
- インタフェースや広告経路のメトリック値を 64 以上にしたい場合，ワイドを選択してください。

IS-IS の広告経路属性には，経路種別，メトリック種別，およびメトリック値の三つがあります。この属性は，広告経路を学習するルータで，学習経路選択時の優先度決定に使用します。

経路広告時にすべての経路属性が付属しているとは限りません。広告経路のプロトコル体系や広告方式により，経路に付属している広告属性と付属していない広告属性が決まっています。

広告内容と広告方式に基づく経路属性の有無，およびその値を次の表に示します。

表 14-3　IS-IS 広告方式と経路属性

広告内容		広告方式	
		ナロウ	ワイド
隣接ルータ	準拠規格	ISO 10589	インターネットドラフト“IS-IS extensions for Traffic Engineering”
	経路種別	広告しない （学習側では内部経路として扱います）	広告しない （学習側では内部経路として扱います）
	メトリック種別	広告しない （学習側ではインターナルメトリックとして扱います）	広告しない （学習側ではインターナルメトリックとして扱います）
	メトリック値	1 ～ 63 (63 以上の値で広告しようとした場合，63 として広告）	1 ～ 16,777,215
IPv4 経路	準拠規格	RFC 1195	インターネットドラフト “IS-IS extensions for Traffic Engineering”
	経路種別	広告する	広告しない （学習側では内部経路として扱います）
	メトリック種別	広告する	広告しない （学習側ではインターナルメトリックとして扱います）
	メトリック値	1 ～ 63 (63 以上の値で広告しようとした場合，63 として広告）	1 ～ 4,261,412,864 (4,261,412,864 以上の値で広告しようとした場合，4,261,412,864 として広告）
IPv6 経路	準拠規格	インターネットドラフト “Routing IPv6 with IS-IS”	
	経路種別	広告する	
	メトリック種別	広告しない （学習側ではインターナルメトリックとして扱います）	
	メトリック値	1 ～ 4,261,412,864 (4,261,412,864 以上の値で広告しようとした場合，4,261,412,864 として広告）	

以下に，IS-IS の広告に付随する各情報を説明します。

- 経路種別
  経路を最初に IS-IS に導入したルータにおいて，その経路が IS-IS 内部由来か，IS-IS 以外のプロトコル由来かを示す情報です。
- メトリック種別
  広告経路のメトリック種別を指定します。メトリック種別には，エクスターナルメトリックと，インターナルメトリックの 2 種類があります。メトリック種別は，広告経路を学習するルータで，ほかの広告経路との経路選択に使用されます。
- メトリック
  広告経路のメトリックを指定します。メトリックは，広告経路を学習するルータで，ほかの広告経路との経路選択に使用されます。

(7) ホスト名広告

本装置では，経路情報の一部として，本装置のホスト名を広告します。本装置が広告したホスト名は，他装置で IS-IS プロトコル情報を表示する際に，本装置を指定するときの本装置名として使用できます。また，表示内容中の本装置名として使用されます。

同様に，他装置がホスト名を広告している場合，本装置の運用コマンドで他装置を指定する場合，他装置の system ID の代わりに他装置名を使用できます。また，本装置運用コマンド表示内容中の他装置の表示が，system ID ではなく他装置名となります。

本装置では，装置名としてコンフィグレーションコマンド system の name パラメータで指定した装置名を広告します。

コンフィグレーションコマンド system の name パラメータ指定がない場合，次に示すホスト名を広告します。

- SB-7800S の場合，文字列「SB-7800S-<system ID>」を広告します。
- SB-5400S の場合，文字列「SB-5400S-<system ID>」を広告します。

14.2.2 エリア分割とレベル

(1) レベルとエリア

IS-IS では，IS-IS ドメインをさらに複数のエリアに分割することができます。IS-IS では，エリア分割を扱うために，レベルという概念を使用します。レベルには，レベル 1 とレベル 2 があります。

レベル 1 は，分割された各エリアのネットワークです。各エリアにはエリア識別子があります。ルータのエリア識別子がエリアのエリア識別子と同じである場合，該当ルータはそのエリアに所属しています。

各エリアのレベル 1 ネットワークを，レベル 1 ドメインと呼びます。各エリアのレベル 1 ドメインは，そのエリアに所属するルータと，そのルータが IS-IS インタフェースにより接続している回線から成り立っています。

IS-IS ドメイン中のレベル 2 ネットワークを，レベル 2 ドメインと呼びます。レベル 2 ドメインは，レベル 2 で動作するルータと，該当ルータにおいてレベル 2 で動作する IS-IS インタフェースにより接続している回線から成り立っています。

レベル 2 ドメインは，分割された各エリア間のルーティングをするためのネットワークです。

IS-IS ルータには，レベル 1 ルータ，レベル 2 ルータ，およびレベル 1-2 ルータがあります。レベル 1 ルータはレベル 1 でだけ動作するルータです。レベル 2 ルータはレベル 2 でだけ動作するルータです。レベル 1-2 ルータはレベル 1 でもレベル 2 でも動作するルータです。本装置は，デフォルトではレベル 1-2 ルータとして動作します。

IS-IS インタフェースには，レベル 1 インタフェース，レベル 2 インタフェース，およびレベル 1-2 インタフェースがあります。レベル 1 インタフェースはレベル 1 でだけ動作する IS-IS インタフェースです。レベル 2 インタフェースはレベル 2 でだけ動作する IS-IS インタフェースです。レベル 1-2 インタフェースはレベル 1 でもレベル 2 でも動作するインタフェースです。本装置のデフォルトでは，IS-IS インタフェースの動作レベルは IS-IS ルータとしての動作レベルに従います。

【注意事項】

1. IS-IS ネットワーク上で，レベル 2 ドメインが二つ以上にならないようにネットワークを構成してください。すべてのレベル 2 で動作しているルータは，レベル 2 で動作しているルータ・インタフェース・回線を経由して接続している必要があります。
   レベル 2 ドメインが二つ以上に分断している場合，経路ができなかったり，誤った経路を導入したりすることがあります。
2. IS-IS ネットワーク上のどのエリアについても，レベル 1 ドメインが二つ以上にならないようにネットワークを構成してください。エリア識別子が同じであるルータは，同一エリアのレベル 1

で動作しているルータ・インタフェース・回線を経由して相互に接続している必要があります。同じエリア識別子のルータからなるネットワークが二つ以上に分断している場合，経路ができなかったり，誤った経路を導入したりすることがあります。

(2) エリア分割時の経路決定

IS-IS では，レベル 1 とレベル 2 とで別個に経路計算を行います。レベル 1 から学習した経路をレベル 1 経路，レベル 2 から学習した経路をレベル 2 経路といいます。

レベル 1-2 ルータでは，レベル 1 経路をレベル 2 へ再配布します。すると，レベル 2 ドメインには，レベル 1-2 ルータを通して接続している全エリア（レベル 1 ドメイン）の経路も再配布されます。結果として，レベル 2 ドメインには，IS-IS ドメイン全体の経路が存在します。

レベル 1-2 ルータでは，デフォルトでは，レベル 2 に存在する経路をレベル 1 へは再配布しません。その代わり，エリア分割している場合に限り，レベル 1-2 ルータはレベル 1 ネットワークへデフォルト経路を広告します。結果として，各エリアのレベル 1 ドメインには，該当エリア内の経路と，レベル 1-2 ルータへのデフォルト経路だけが存在します。

ただし，学習ルータがレベル 1-2 ルータである場合，ほかのレベル 1-2 ルータの広告したデフォルト経路を学習しません。エリア分割時のデフォルト経路を学習するのは，レベル 1 ルータだけとなります。

エリア分割をしない場合のネットワーク構成例を次に示します。

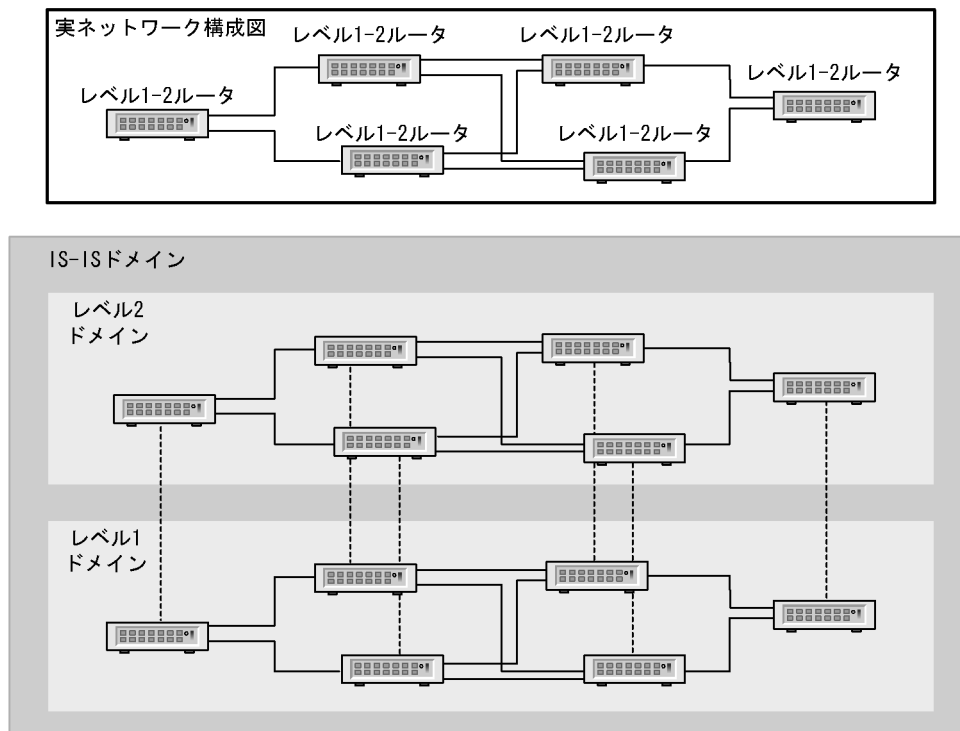
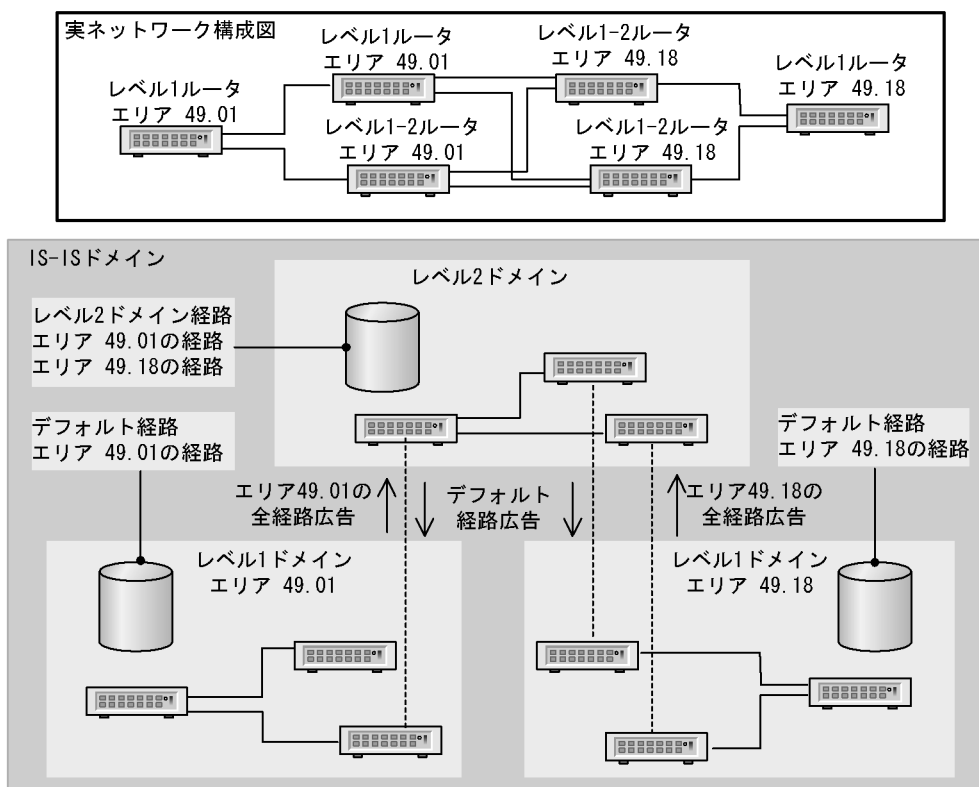
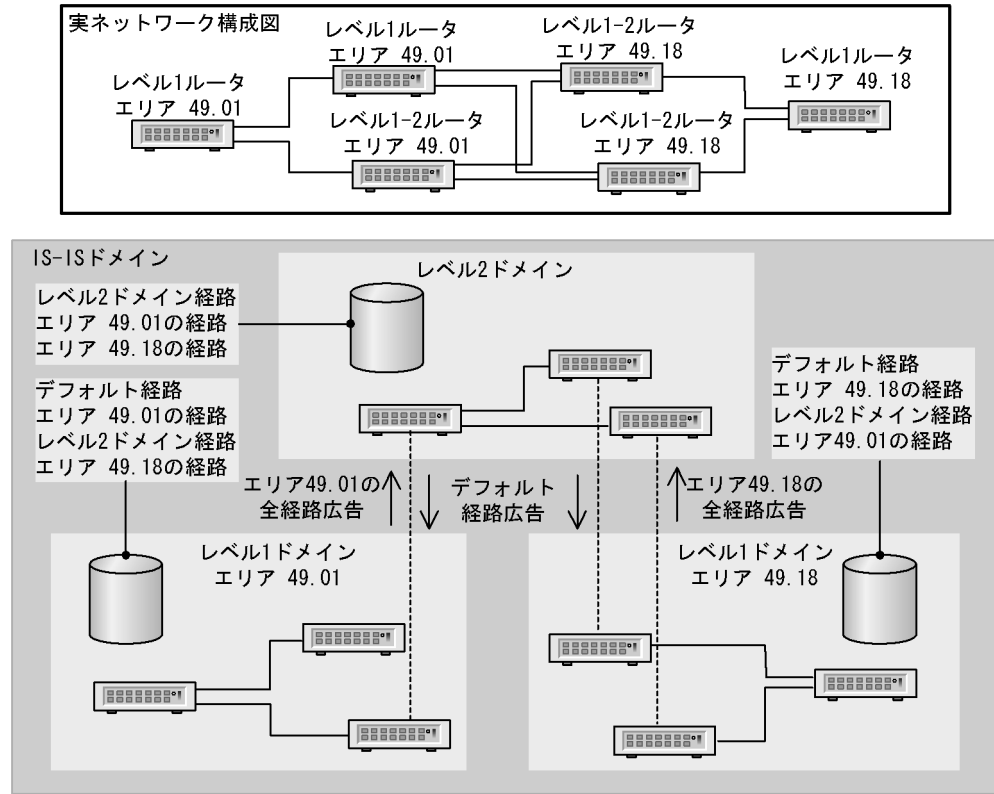
図 14-2　エリア分割をしない場合のレベル別動作例

エリア分割の例とその場合の経路モデルを次に示します。

図 14-3 エリア分割時のレベル別動作例

(3) ドメイン全体への経路配布(ドメインワイド)

本装置では，レベル 2 ネットワーク上の経路をレベル 1 へ再配布する拡張機能をサポートしています。この機能により，レベル 1 ネットワーク上での IS-IS ドメイン全体の経路を生成することができます。

ドメインワイド適用例を次に示します。

この機能は，エキスポート・フィルタ(経路再配布定義)により，IS-IS レベル 2 経路を IS-IS レベル 1 へ再配布するよう定義することにより，有効になります。レベル 2 経路を基に再配布されたレベル 1 経路のことを，ダウン経路といいます。

図 14-4　ドメインワイド適用時の経路モデル

(4) レベル間再配布時の経路属性

レベル 1-2 ルータでは，デフォルトでレベル 1 学習経路をレベル 2 へ再配布します。また，ドメインワイド設定をした場合には，レベル 2 学習経路をレベル 1 へ再配布します。レベル間経路の再配布に当たり，特に設定をしない限り，経路の属性（メトリック，メトリック種別，経路種別）を引き継いで広告します。

レベル 1 学習経路をレベル 1 へ再配布することはできません。また，レベル 2 学習経路をレベル 2 へ再配布することはできません。

14.2.3 経路選択アルゴリズム

IS-IS では，IS-IS ドメイン上で広告されている同一宛先への経路情報が複数ある場合，「表 14-4　IS-IS の経路優先順位」に示す決定優先順位に従い，優先経路を決定・選択します。

すべての条件において，条件の等しい経路が複数あり，これがほかの経路と比較して最優先である場合，この複数の経路をすべて選択します。この複数の経路を，イコールコストマルチパスと呼びます。本装置では，優先経路がイコールコストマルチパスであった場合，IS-IS のマルチパス設定が有効であった場合にだけ，マルチパスを採用します。IS-IS のマルチパス設定が無効である場合，マルチパスの中から 1 経路を選択します。

表 14-4　IS-IS の経路優先順位

選択条件の優先順位	経路属性	比較方法
高 ↑	メトリック種別	メトリック種別がインターナルメトリックである経路をエクスターナルメトリックである経路より優先します

選択条件の優先順位	経路属性	比較方法
	経路学習元レベルダウン経路	以下の順で選択します。 1. レベル 1 経路 2. レベル 2 経路 3. レベル 1 ダウン経路
↓	エクスターナル メトリック時の 広告メトリック値	メトリック種別がエクスターナルメトリックである場合，広告メトリックの小さい経路を選択します。
低	インターナルメトリック値	インターナルメトリックの小さい経路を選択します。

(1) メトリック種別

IS-IS の広告経路には，メトリックが指定してあります。IS-IS では，経路の広告メトリックに種別があります。メトリック種別には，エクスターナルメトリックとインターナルメトリックがあります。

メトリック種別がインターナルメトリックである経路は，メトリック種別がエクスターナルメトリックである経路よりも優先して選択されます。

(2) 学習元レベル・ダウン経路

レベル 1 へ配布された経路を学習する場合，この経路はレベル 1 経路になります。レベル 2 へ配布された経路を学習する場合，この経路はレベル 2 経路になります。

レベル 1-2 ルータがレベル 2 で学習しレベル 1 へ再配布した経路を学習する場合，この経路はレベル 1 ダウン経路になります。

ダウンでない経路は，ダウン経路よりも優先して選択されます。ダウンでない経路については，レベル 1 経路をレベル 2 経路よりも優先して選択します。

(3) エクスターナルメトリック比較

比較経路の両方にエクスターナルメトリックと指定してある場合，広告メトリックの小さい経路を，広告メトリックの大きい経路よりも優先して選択します。

(4) インターナルメトリック比較

学習経路のインターナルメトリックの小さい経路を，インターナルメトリックの大きい経路よりも優先して選択します。

広告経路のメトリック種別がインターナルメトリックである場合，学習経路のインターナルメトリックは，経路学習ルータから経路広告ルータまでの最短経路のメトリック（経路上にある各ルータの出力インタフェースのメトリックの総和）と，広告経路のメトリックの和です。

広告経路のメトリック種別がエクスターナルメトリックである場合，学習経路のインターナルメトリックは，経路広告ルータまでの最短経路のメトリックです。

14.2.4 経路学習

(1) 経路導入

経路種別（内部経路・外部経路）は，IS-IS の経路選択アルゴリズムには影響しません。しかし，本装置のルーティングテーブルに導入するときの優先度（プリファレンス値）が異なります。なお，内部経路と外部経路がマルチパスである場合は，プリファレンス値は内部経路扱いとなります。

複数のルーティング種別が同時動作するとき，それぞれは独立した経路選択手順に従い，ある宛先アドレ

スへの経路情報から一つの最良の経路を選択します。その結果，ルータ内ではある宛先アドレスへの経路情報が複数導入されます。このような場合，それぞれの経路情報のプリファレンス値が比較されて優先度の高い経路を学習します。IS-IS 経路を学習した後，IS-IS より優先度の低い経路を IS-IS で広告することはできません。

（2） プリファレンス値

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコルごとに生成する経路情報のデフォルトのプリファレンス（優先度）値をコンフィグレーションで設定できます。なお，プリファレンスは値の小さい方の優先度が高くなります。各プロトコルのプリファレンスのデフォルト値を次の表に示します。

表 14-5　プリファレンスのデフォルト値

経路	デフォルトプリファレンス値
直結経路	0（固定値）
OSPF/OSPFv3 の AS 内経路	10
IS-IS の内部経路	15
スタティック経路	60
RIP/RIPng 経路	100
集約経路	130
OSPF/OSPFv3 の AS 外経路	150
IS-IS の外部経路	160
BGP4/BGP4+ 経路	170
DHCP のデフォルト経路※	200

注※　DHCP サーバから割り当てられたデフォルト経路です。

14.2.5　認証 (IS-IS)

IS-IS には，受信パケットを認証する機能があります。認証機能により，一部の攻撃を防ぐことができます。

- ネットワーク上に不正に IS-IS プロトコルを送受信する機器が存在しても，認証鍵が一致しない限り，この機器と接続しないよう動作します。
- ネットワーク上に存在する攻撃者の機器が，ネットワーク上にすでに存在し接続している正しいルータのふりをして LSP を送信してきても，不正機器の認証鍵が一致しない限り，この LSP を無視します。

IS-IS 認証の認証対象は二つあります。それぞれ隣接ルータと LSP です。

本装置がサポートする IS-IS 認証方式は二つあります。それぞれ，平文認証と暗号化認証です。

（1） 隣接ルータの認証

隣接ルータへ接続している本装置のインタフェースに設定した認証鍵と，本装置へ接続している隣接ルータのインタフェースに設定した認証鍵が同じ場合にだけ，本装置と隣接ルータが互いに認証に成功し，接続することができます。

ブロードキャスト型インタフェースでは，レベル個別に認証します。ポイント - ポイント型インタフェースでは，レベルを区別せずに隣接ルータを認証します。

【注意事項】

1. ブロードキャスト型インタフェースの場合
   ある回線に接続しているすべてのルータで，その回線への接続 IS-IS インタフェースのレベル 1 接続ルータ認証鍵を一致させてください。また，その回線への接続 IS-IS インタフェースのレベル 2 隣接ルータ認証鍵を一致させてください。認証鍵が一致していない場合，隣接ルータとつながりません。
2. ポイント - ポイント型インタフェースの場合
   対向装置と同じ認証鍵をレベル指定なしで設定してください。認証鍵が一致していない場合，隣接ルータとつながりません。
   認証鍵をレベル指定して設定した場合，レベル 1-2 インタフェースまたはレベル 1 インタフェースではレベル 1 の認証鍵を使用します。レベル 2 インタフェースではレベル 2 の認証鍵を使用します。

(2) LSP の認証

LSP の生成元ルータに設定した認証鍵と，本装置に設定した認証鍵が同じ場合だけ，本装置が該当 LSP を受け入れます。逆に，本装置に設定した認証鍵と，IS-IS ネットワーク上のほかのルータに設定した認証鍵が同じ場合だけ，本装置が生成した LSP がほかのルータに受け入れられます。

【注意事項】

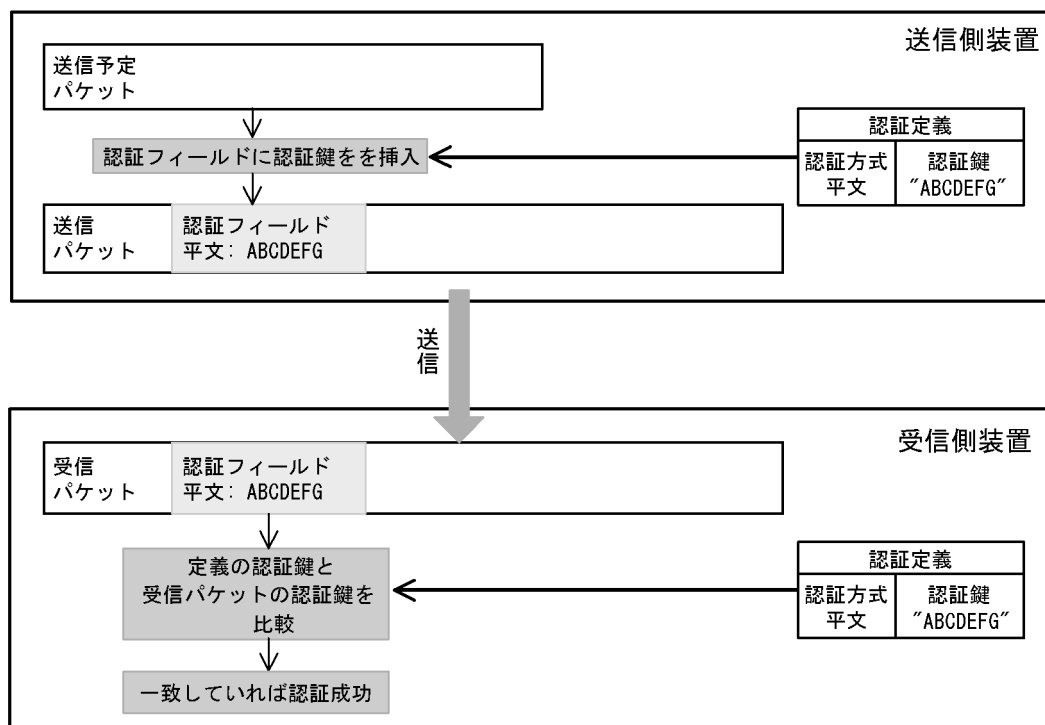
1. レベル 1 ドメイン上にあるすべてのルータで，レベル 1 の LSP 認証鍵を一致させてください。一致していない場合，レベル 1 の経路が正しく生成されません。
2. IS-IS ドメイン上にあるすべてのレベル 2 ルータで，レベル 2 の認証鍵を一致させてください。一致していない場合，レベル 2 の経路が正しく生成されません。

(3) 平文認証

平文認証は，認証鍵がそのままの形でパケットに含まれる方式です。平文認証のモデル図を次に示します。

送信・広告側では認証鍵をパケットの認証フィールドにコピーします。受信側では，認証鍵とパケット中の認証フィールドを比較し，これが一致したときだけ認証に成功したものとみなします。

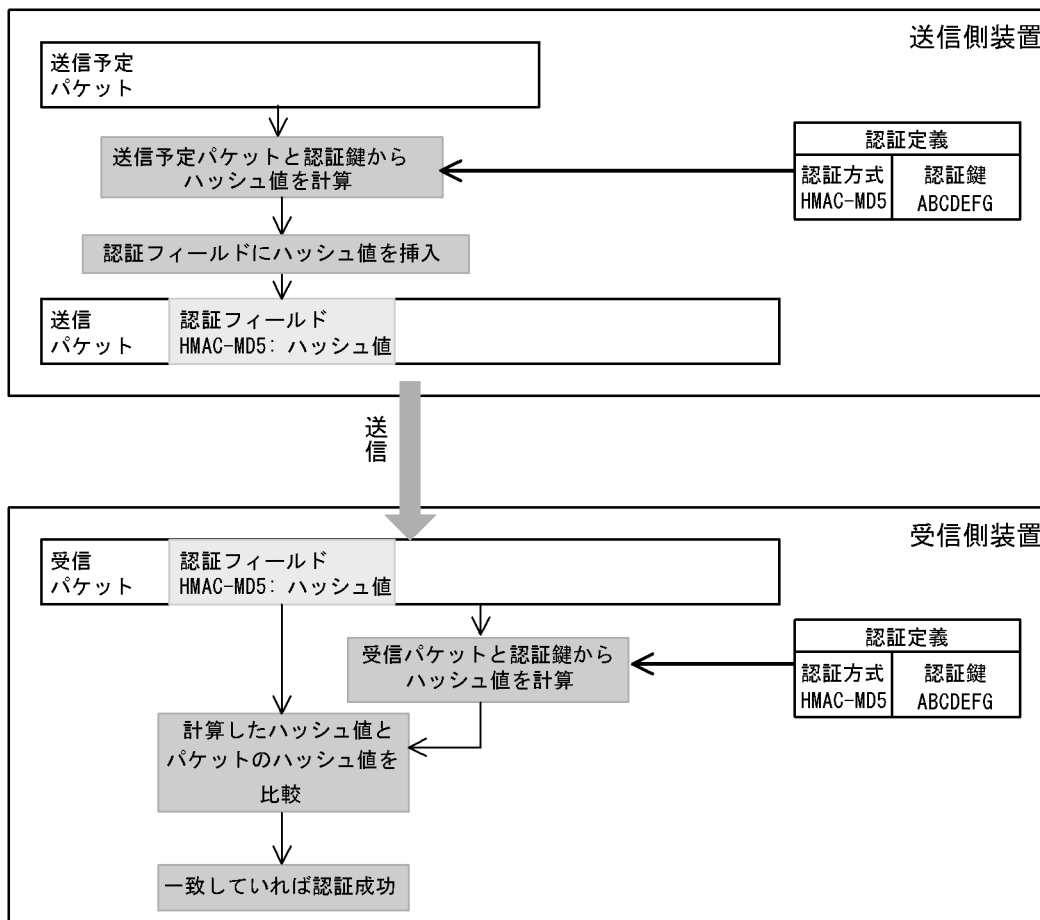
認証方式の不一致，認証鍵長の不一致，および認証鍵の不一致は，すべて認証失敗とみなします。

図 14-5　平文認証のモデル図

（4） HMAC-MD5 認証

HMAC-MD5 認証は，パケットと認証鍵を基に HMAC-MD5 ハッシュ関数を実行し，その結果得られるハッシュ値がパケットに含まれる方式です。HMAC-MD5 認証のモデル図を次に示します。

送信・広告側では，パケットと認証鍵を基に HMAC-MD5 ハッシュ値を求め，これをパケットの認証フィールドにコピーします。受信側では，受信パケットと認証鍵を元に HMAC-MD5 ハッシュ値を求め，ハッシュ値とパケット中の認証フィールドの値を比較し，これが一致したときだけ認証に成功したものとみなします。

認証方式の不一致，およびハッシュ値の不一致は，認証失敗とみなします。

図 14-6　HMAC-MD5 認証のモデル図

（5） 認証の変更

本装置では，受信時の認証確認を行わず，常に認証に成功したことにするコンフィグレーションオプションをサポートします。認証鍵や認証方式を変更する場合，このオプションを使用し，以下の手順で運用してください。これにより，設定変更をルータ 1 台ずつ行い，かつ IS-IS プロトコル通信を切断することなく，認証設定を変更することができます。

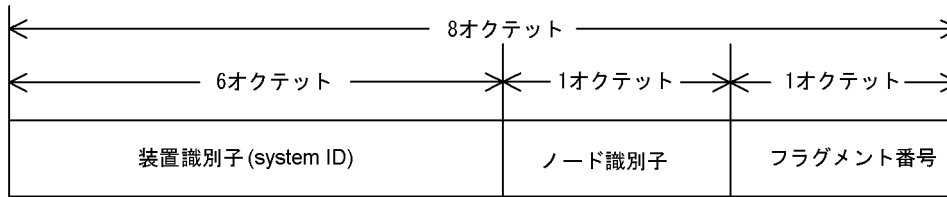
1. まず，認証変更対象の全ルータについて，1 台ずつ順に「認証確認しない」オプションを設定します。
2. ついで，認証変更対象の全ルータについて，1 台ずつ順に認証設定を変更します。
3. 最後に，認証変更対象の全ルータについて，1 台ずつ順に「認証確認しない」オプション設定を削除します。

14.2.6　IS-IS 詳細

（1） LSP

LSP は，1 台のルータ当たり，1 レベル当たり，256 個生成することができます。LSP は，1 パケット当たり最大 1492 オクテットです。

LSP にはそれぞれ LSP を識別するための識別子，LSPID が振ってあります。LSPID のフォーマットを次に示します。

図 14-7　LSPID フォーマット

- 装置識別子
  LSP 生成もとの装置識別子です。
- ノード識別子
  装置以外に LSP を生成する broadcast 型 OSI ネットワークと区別するための識別子です。ルータ自体の LSP は，この値が 0 になります。
- フラグメント番号
  同一ルータ上の 256 個の LSP を区別するための番号です。

LSP には，その新しさを示すシーケンスナンバー (Sequence Number) があります。最初に LSP を生成するときのシーケンスナンバーは 1 です。情報の追加・削除・変更により LSP を作り直すたびに，シーケンスナンバーが 1 増えます。2 台のルータ間で同一 LSP のシーケンスナンバーが異なる場合，シーケンスナンバーの大きな LSP をより新しいとみなします。

LSP には，27 オクテットのヘッダと，TLV と呼ばれるフィールドが多数含まれています。TLV には，生成元ルータについての各種情報が含まれています。TLV の種別・名前，および広告内容を次の表に示します。

TLV フィールドは，以下の三つのフィールドから成り立っています。

1. タイプ
   値フィールドに入っている情報の種別を示すフィールドです。長さは 1 オクテットです。0 以上 255 以下の値をとります。
2. 長さ
   値フィールドの長さを示すフィールドです。このフィールドの長さは 1 オクテットです。0 以上 255 以下の値をとります。値の単位はオクテットです。
3. 値
   タイプフィールドに示した種類の広告内容を納めるフィールドです。

表 14-6　TLV の種別

TLV 種別名	タイプ	説明	広告方式 (ナロウ・ワイド)	情報一つ当たりの長さ (オクテット)	本装置のサポート
Area Addresses	1	このルータの所属するエリアアドレス	両方に含まれる	エリアアドレスの長さ + 1 (可変長)	サポート
Intermediate System Neighbours	2	このルータと接続している隣接ルータ	ナロウだけ	11	サポート
End System Neighbours	3	このルータと接続している OSI ホスト機器	両方に含まれる	-	未サポート
Partition Designated Level 2 Intermediate System	4	エリアが分断されたときの，分断範囲内の代表ルータ	両方に含まれる	-	未サポート

TLV 種別名	タイプ	説明	広告方式 (ナロウ・ワイド)	情報一つ当たりの長さ (オクテット)	本装置のサポート
Prefix Neighbours	5	このルータが広告している OSI 経路宛先	両方に含まれる	-	未サポート
Authentication Information	10	LSP の認証情報	両方に含まれる	認証の設定による (可変長)	サポート
Optional Checksum	12	LSP のチェックサム	両方に含まれる	2	未サポート
extended IS reachability	22	TE (トラフィック・エンジニアリング) 情報を含む，隣接ルータ情報	ワイドだけ	11 + TE 情報長 (可変長)	メトリック拡張だけサポート
IP Internal Reachability Information	128	このルータが広告する IPv4 内部経路	ナロウだけ	12	サポート
Protocol Supported	129	このルータのサポートプロトコル体系	両方に含まれる	1	サポート
IP External Reachability Information	130	このルータが広告する IPv4 外部経路	ナロウだけ	12	サポート
Inter-Domain Routing Protocol Information	131	IS-IS ドメイン外ルーティングプロトコルの追加情報	両方に含まれる	規定なし	未サポート
IP Interface Address	132	IPv4 インタフェースアドレス	両方に含まれる	4	サポート
Traffic Engineering router ID	134	TE で使用するこのルータのルータ ID	両方に含まれる	4	未サポート
extended IP reachability	135	TE 情報を含む，IPv4 経路情報	ワイドだけ	5 + 宛先アドレス長 + TE 情報長 (可変長)	メトリック拡張だけサポート
Dynamic Hostname	137	このルータの装置名	両方に含まれる	名前の長さ (可変長)	サポート
IPv6 Interface Address	232	IPv6 インタフェースアドレス	両方に含まれる	16	サポート
IPv6 Reachability	236	IPv6 経路情報	両方に含まれる	8 + 宛先アドレス長 + TE 情報長 (可変長)	サポート

（凡例） - : 該当しない

(2) IS-IS インタフェースと隣接ルータ認識

IS-IS では，インタフェースから定期的に IS-IS Hello PDU (IIH) というパケットを送信しています。対向装置から IIH パケットを受信すると，対向装置を隣接ルータとして認識します。

IIH パケットには，パケットの有効時間 (ホールドタイマ) が含まれています。IIH を受信してからホールドタイマの時間 (単位 : 秒) の間，隣接ルータを認識しつづけます。通常，ホールドタイマは IIH パケットの送信間隔よりも十分に長いため，IIH パケットを受信しつづける限り，隣接ルータとの接続が途絶えることはありません。

本装置が IS-IS プロトコルを交換するためには，IS-IS インタフェースが以下の条件を満たす必要がありま

す。

- 該当インタフェースが OSI パケット送受信をサポートしていること。
- 該当インタフェースの OSI パケット送受信上の MTU が，1492 オクテット以上であること。
- 該当インタフェースが，本装置のサポートするプロトコル体系のパケット送受信をサポートしていること。

IIH パケットを受信したときに，対向装置を隣接ルータとして受け入れるためには，以下の条件を満たす必要があります。

- 本装置の該当インタフェースに認証設定がある場合，認証に成功すること。
- 本装置のルーティングサポートプロトコル体系全てを，対向装置がサポートしていること。
- 本装置のサポートプロトコル体系について，対向装置に適切なインタフェースアドレスが存在すること。
  IPv4 の場合，本装置のインタフェースネットマスクと，対向装置のインタフェースアドレスが一致する必要があります。
  IPv6 の場合，対向装置にリンクローカルアドレスが存在する必要があります。
- 本装置と対向装置との間で，インタフェースに一致する動作レベルがあること。
  例えば，本装置インタフェースがレベル 1 インタフェース，対向装置インタフェースがレベル 2 インタフェースである場合，本装置・対向装置間は隣接ルータとして接続できません。
- レベル 1 の場合には，本装置に設定のエリアアドレスと対向装置に設定のエリアアドレスとの間に，共通するエリアアドレスがあること。
  エリアアドレスの異なるルータ間は，レベル 1 では接続できません。

本装置では，IIH パケット送信間隔，および IIH パケット送信間隔とホールドタイマの比を設定できます。デフォルトでは，IIH パケット送信間隔は 10 秒，ホールドタイマ比は 3 倍です。このとき，ホールドタイマは 30 秒になります。

ただし，本装置が代表ルータとなっているインタフェースについてだけ，IIH パケット送信間隔に，IIH パケット送信間隔として設定した値をホールドタイマ比で割った値を使用します。この場合，デフォルトでは，IIH パケット送信間隔は 3 秒，ホールドタイマは 9 秒になります。

(3) 経路広告

IS-IS への経路広告の要因と，経路広告情報の詳細を以下に示します。

経路広告情報を LSP に追加する際，プロトコル体系 (IPv4・IPv6) や，広告方式 (ナロウ・ワイド) によって，広告できない情報やメトリック値の切り詰めが発生します。詳細は「表 14-3　IS-IS 広告方式と経路属性」をご参照ください。

- IS-IS インタフェースのネットワークアドレス (IPv4) およびプレフィックス (IPv6)
  IS-IS では，アップ状態にある IS-IS インタフェースのネットワークアドレス，およびプレフィックスを，IS-IS インタフェース動作レベルの LSP に追加します。

IS-IS インタフェースのネットワークアドレス・プレフィックス広告時のデフォルト値を次の表に示します。

表 14-7　IS-IS インタフェースのネットワークアドレス・プレフィックス広告時のデフォルト値

広告パラメータ	デフォルト値	フィルタによる変更
広告する・しない	する	不可能

広告パラメータ		デフォルト値	フィルタによる変更
IS-IS 経路集約の対象になる・ならない		• レベル 1 インタフェース →集約されない • レベル 2 インタフェース →集約されない • レベル 1-2 インタフェース →レベル 1 は集約されない レベル 2 は集約される	不可能
広告先レベル		• レベル 1 インタフェース →レベル 1 • レベル 2 インタフェース →レベル 2 • レベル 1-2 インタフェース →レベル 1 とレベル 2 の両方	不可能
広告属性	経路種別	内部経路	不可能
	メトリック種別	インターナルメトリック	不可能
	メトリック値	IS-IS インタフェースのメトリック値 (デフォルト:10)	不可能※
	ダウン	ダウン経路にはならない	不可能

注※　IS-IS インタフェースの該当レベルのメトリックを変更することで，変更可能です。

- IS-IS レベル間経路広告

  IS-IS では，あるレベルで学習した経路を別のレベルへ再広告することができます。

  エキスポート・フィルタを設定することにより，レベル間の再広告の有無，および一部の広告パラメータを制御することができます。デフォルトでは，レベル 1 で学習した経路をレベル 2 へ再広告します（レベル 2 で学習した経路はレベル 1 へ再広告しません)。

  なお，IS-IS レベル 1 経路をレベル 1 へ再広告することはできません。また，レベル 2 経路をレベル 2 へ再広告することもできません。

  レベル間経路広告のデフォルト値とエキスポート・フィルタによる変更を，次の表に示します。

表 14-8　IS-IS レベル間経路再広告時のデフォルト値とエキスポート・フィルタによる変更

広告パラメータ		デフォルト値	フィルタによる変更
再配布をする・しない		レベル 1 経路をレベル 2 へ再配布する	可能
IS-IS 経路集約の対象になる・ならない		再配布経路が集約される	不可能
広告先レベル		レベル 2 （レベル 2 が動作していない場合，レベル 1)	可能（ただし，学習元と同一レベルには広告しない）
広告属性	経路種別	再配布元経路の属性を引き継ぎます	メトリック種別を指定した場合，外部経路となります
	メトリック種別	再配布元経路の属性を引き継ぎます	可能
	メトリック値	再配布元経路の属性を引き継ぎます	可能
	ダウン	• 再配布元経路がレベル 1 経路→レベル 2 経路 • 再配布元経路がレベル 2 経路→レベル 1 ダウン経路	不可能

- レベル 2 からレベル 1 へのデフォルト経路

レベル 1-2 ルータで，エリア分割時にレベル 1 へ広告するデフォルト経路は，LSP ヘッダ中のフィールド’attached bit’により広告されます。経路種別・メトリック種別・メトリック値すべて広告しません。学習時には，内部経路・インターナルメトリック・メトリック値 0 とみなします。

表 14-9　レベル 1 のデフォルト経路のデフォルト値とエキスポート・フィルタによる変更

広告パラメータ		デフォルト値	フィルタによる変更
再配布をする・しない		• レベル 1 ルータであるか，レベル 2 ルータである →しない • レベル分割を適用していない →しない • レベル 1-2 ルータであり，IS-IS ドメインがレベル分割されている →する	不可能
IS-IS 経路集約の対象になる・ならない		集約されない	不可能
広告先レベル		レベル 1	不可能
広告属性	経路種別	内部経路	不可能
	メトリック種別	インターナルメトリック	不可能
	メトリック値	0	不可能
	ダウン	レベル 1 ダウン経路	不可能

- 他プロトコル経路再配布
  エキスポート・フィルタを定義してある場合，フィルタに従い，他プロトコル経路をフィルタで指定したレベルの LSP に追加します。メトリック種別とメトリック値については，エキスポート・フィルタにより変更可能です。付加情報のデフォルト値を次の表に示します。

表 14-10　IS-IS 経路再配布時のデフォルト値とエキスポート・フィルタによる変更

広告パラメータ		デフォルト値	フィルタによる変更
再配布をする・しない		しない	可能
IS-IS 経路集約の対象になる・ならない		フィルタによる再配布経路が集約される	不可能
広告先レベル		レベル 2 （レベル 2 が動作していない場合，レベル 1）	可能（片方または両方）
広告属性	経路種別	外部経路	不可能
	メトリック種別	インターナルメトリック	可能
	メトリック値	• 再配布元経路にメトリックがない場合 →メトリック 10 で広告します • 再配布元経路のメトリックが 0 である場合 →メトリック 10 で広告します • 上記に該当しない場合 →再配布元経路のメトリックを引き継ぎます	可能
	ダウン	ダウン経路にならない	不可能

（4） 広告経路集約 (サマリー)

IS-IS では，多数の広告経路を，その経路宛先を包含するひとつのネットワークアドレス・プレフィックスに集約して広告することができます。この機能をサマリーと呼びます。

サマリーするネットワークアドレス・プレフィックスを指定した場合，これに包含される宛先への経路広

告は全て削除され，その代わりにサマリーのネットワークアドレス・プレフィックスが広告されます。このとき，付加情報は，集約において最短である経路の付加情報を使用します。経路広告集約時の選択アルゴリズムを次の表に示します。

表 14-11　経路集約時の経路属性引き継ぎ元経路選択条件の優先順位

選択条件の優先順位	名前	比較方法
高	経路種別	内部経路を優先します。
↑	メトリック種別	メトリック種別がインターナルメトリックである経路を選択します。
	エクスターナル メトリック時の広告メトリック値	メトリック種別がエクスターナルメトリックである場合，広告メトリックの小さい経路を選択します。
↓ 低	インターナルメトリック値	インターナルメトリックの小さい経路を選択します。

(5) LSP の交換と同期

IS-IS では，隣接ルータとの間で，互いに所持していない LSP を送信しあいます。新たに LSP を生成または受信した場合，これを全隣接ルータに送信します。これにより，本装置と隣接ルータとの間で，同じ LSP の集合を保持するようにします。これを LSP の同期といいます。

LSP 同期手順により，本装置の LSP は全ての隣接ルータに送信されます。また，隣接ルータでは，隣接ルータのすべての隣接ルータに本装置の LSP を送信します。隣接ルータの隣接ルータでは，さらにその全隣接ルータに LSP を送信します。この手順により，本装置の LSP は該当レベルドメイン上の全ルータに配布されます。また，そのレベルのドメイン上にある全ルータ LSP が本装置に集まります。

point-to-point，および generic topology 型の OSI インタフェースでは，LSP の同期を以下の手順で行います。

1. 隣接ルータ認識時に，本装置の全 LSP の LSPID を列挙したパケット (CSNP: Complete Sequence Numbers PDU) を送信します。
   隣接ルータからも，隣接ルータの全 LSP の LSPID を列挙した CSNP が送信されてきます。
2. 隣接ルータの CSNP 中に本装置が保持していない LSP の LSPID が含まれている場合，LSP 更新を示すパケット (PSNP: Partial Sequence Numbers PDU) を使用して送信します。このとき，該当 LSP の LSPID について，LSP のバージョンを 0 として送信します。
3. 隣接ルータが PSNP を受信すると，本装置が所持している LSP が，隣接ルータの所持している LSP よりもバージョンが古い (小さい) ことがわかります。これに基づき，隣接ルータは該当 LSP を送信します。
4. 本装置が LSP を受信し，これを LSP データベースに保持します。該当隣接ルータ以外にも隣接ルータが存在する場合，受信した LSP の LSPID とそのバージョンを，PSNP でほかの隣接ルータへ送信します。

broadcast 型の OSI インタフェースでは，LSP の同期を以下の手順で行います。

1. まず，インタフェース上にある隣接ルータと本装置の中から，代表ルータ (DIS: Designated IS) を 1 台選択します。
2. 代表ルータは，定期的に代表ルータの保持する全 LSP の LSPID を CSNP によりブロードキャストで送信します。
3. CSNP を受信したルータにおいて CSNP に含まれる LSPID を保持していない場合，その LSPID を，LSP のバージョンを 0 として PSNP でブロードキャストで送信します。

4. CSNP を受信したルータにおいて CSNP に含まれる LSPID のバージョンの方が保持している LSPID のバージョンよりも新しい場合，その LSPID を，受信ルータの保持する LSP バージョンで PSNP でブロードキャストで送信します。
5. CSNP または PSNP を受信したルータにおいて，含まれている LSPID のバージョンが保持しているバージョンよりも古い場合，該当 LSP をブロードキャストで送信します。
6. LSP を受信した場合，これが保持する LSP よりも新しければ，LSP データベースに保持します。受信ルータに他に IS-IS インタフェースが存在する場合，ほかのインタフェース上にある隣接ルータへ，受信した LSP の LSPID とそのバージョンを，PSNP でほかの隣接ルータへ送信します。

(6) 経路計算

IS-IS では，LSP データベース上の LSP が更新されたときに経路計算を行います。経路計算は，まずレベルごとに別個に行います。経路計算の手順は以下のとおりです。

1. LSP データベースから隣接ルータ情報を抜き出し，ドメイン上の IS-IS ルータと隣接関係からなるネットワーク構成図 (トポロジ) を書き出します。
2. 書き出したネットワーク構成図と，そこに書いてあるルータ間のメトリックから，ネットワーク上の全ルータへの最短経路を計算します。短いとは，メトリックが小さいことを指します。最短経路が複数ある場合，そのルータへのネクストホップは複数になります (マルチパス)。
3. 次に，最短経路が求まった全ルータについて，そのルータが LSP に広告している全経路を取り出します。
4. 同じ経路を広告しているルータが複数ある場合，「14.2.3　経路選択アルゴリズム」に記述のアルゴリズムに従い，最短経路を選び出します。最短経路を広告しているルータが複数ある場合，最短経路はマルチパスになります。

経路計算によりレベル別経路を計算後，レベル別の経路を統合して，以下の規則によって IS-IS としての最短経路を選択します。

- ある宛先への経路が一方のレベルにしかない場合，この経路を採用します。
- ある宛先への経路が両方のレベルにある場合，「14.2.3　経路選択アルゴリズム」に記述のアルゴリズムに従い，最短経路を選び出します。自ルータが広告している経路が最短経路である場合，経路は学習しません。必ず長短が決定するので，レベル 1 とレベル 2 との間でマルチパスになることはありません。

14.2.7 オーバロードビット

(1) 概要

隣接ルータとの接続・LSP の同期などが完了していなかったり，安定していなかったりすると，ネットワーク全体のルーティングが不安定になることがあります。ルータの起動時・再起動時やネットワークにルータを追加するときに，このような状況がおこることがあります。

本装置では，広告する LSP のオーバロードビットを 1 にすることで，本装置をルーティングに使用しないように広告することができます。また，オーバロードビット広告時にグレースフル・スタートによる隣接ルータ広告を抑止するかどうかを選択できます。

本装置の LSP のオーバロードビットを 1 にすると，ほかのルータは本装置に隣接しているルータがないものとして経路を計算します。この結果，それぞれのレベルで，本装置以外のルータが広告した宛先への経路が本装置を迂回します。迂回できない場合は，経路がなくなり通信できなくなります。本装置が広告している宛先へは，通常通り経路ができて通信できます。

グレースフル・スタートを併用すると，隣接ルータに隣接接続を広告させないようにできます。この結果，ほかのルータが経路を計算するときに本装置自体を除きます。このため，本装置が広告している宛先とも

通信できなくなります。

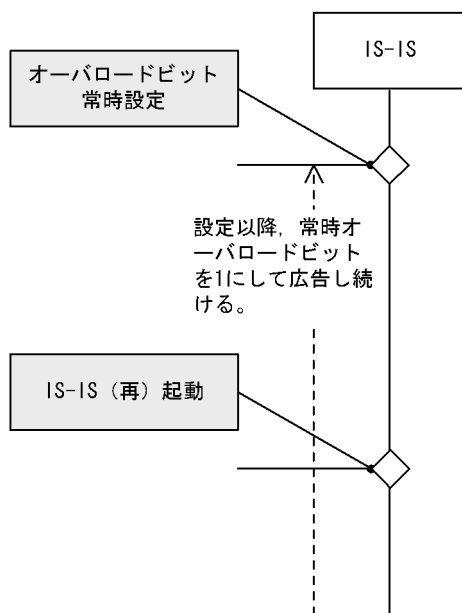
本装置の装置アドレスによる通信は，IS-IS が装置アドレスを広告することによってできるようになります。このため，装置アドレスを使った telnet・SNMP による管理や BGP による経路交換は，オーバロードビットだけを使用した場合はできますが，グレースフル・スタートを併用するとできなくなります。

一方，本装置が広告している経路の代替経路をほかのルータが広告している場合，オーバロードビットだけを使用していると，本装置の経路を使用するおそれがあります。グレースフル・スタートを併用すれば，必ず代替経路を選択することになります。

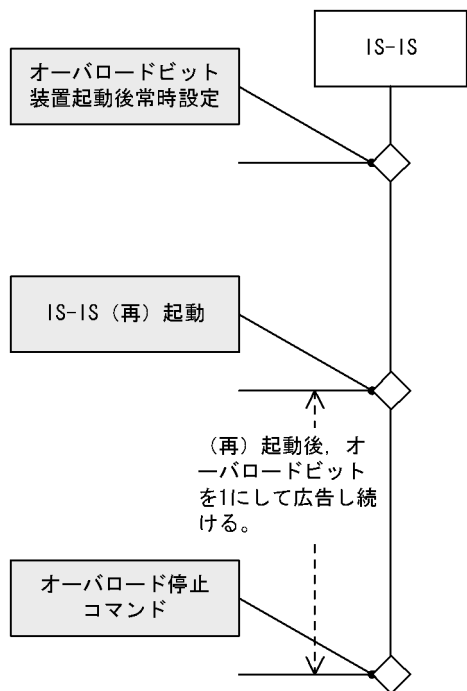
本装置では，オーバロードビットを広告する条件を，次に示す三つから選択できます。

● **常時**

常時，オーバロードビットを 1 にして LSP を広告します。動作手順を次の図に示します。
ネットワークに装置を追加する時や，ネットワークから装置を取り除く時に使用します。

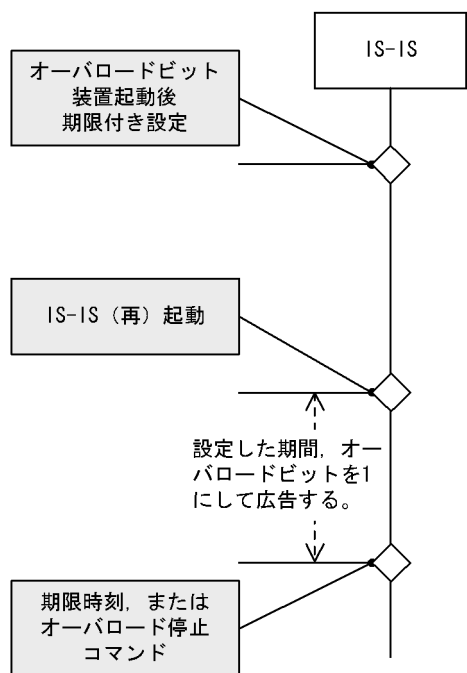
図 14-8　常時設定時の動作手順

● **装置起動後常時**

装置の起動・再起動・系切替（グレースフル・リスタート成功時を除く）後，オーバロードビットを 1 にして LSP を広告します。定義を削除するか，オーバロード広告停止の運用コマンドを実行するまで，この広告が継続します。動作手順を次の図に示します。
装置が起動・再起動したときに，運用者が状態の安定を確認してからルーティングを開始したい場合に使用します。

図 14-9 装置起動後常時設定時の動作手順

● 装置起動後，期限付き

装置の起動・再起動・系切替（グレースフル・リスタート成功時を除く）後，オーバロードビットを 1 にして LSP を広告します。設定した期限を経過するか，オーバロード広告停止運用コマンドを実行するまで，この広告が継続します。動作手順を次の図に示します。

装置が起動・再起動したときにルーティングを抑止して，その後自動的に復旧するのが望ましい場合に使用します。

図 14-10 装置起動後期限付き設定時の動作手順

【注意事項】

1. 本装置がレベル 1-2 ルータの場合，デフォルトでレベル 1 学習経路をレベル 2 へ再配布するため，オーバロードビットを 1 にしてもほかのルータでは該当経路を経路計算から除きません。これは，IS-IS レベル間経路広告の宛先を本装置の LSP で広告するためです。
2. グレースフル・スタートを使用するためには，隣接ルータ上で RFC 3847 に規定してあるグレースフル・リスタートのヘルパー機能が動作している必要があります。これは規格上，グレースフル・スタート機能がグレースフル・リスタート機能の一部であるためです。隣接ルータがヘルパー機能をサポートしていない場合，グレースフル・スタートは機能しません。
3. グレースフル・スタートを使用する場合，ブロードキャスト型ネットワークにある隣接ルータのプライオリティ値を 1 以上に設定してください。これは，グレースフル・スタートを併用している場合，オーバロード広告中は本装置が代表ルータにならないように，本装置のブロードキャスト型回線のプライオリティ値を 0 にするからです。

14.2.8　グレースフル・リスタート

(1) 概要

グレースフル・リスタートは，装置の BCU が系切替したり，運用コマンドなどによってルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機能です。グレースフル・リスタート機能一般については，「12.8　グレースフル・リスタートの概要」を参照してください。

IS-IS では，グレースフル・リスタートによって IS-IS の再起動を行う装置のことをリスタートルータといいます。リスタートルータにあるグレースフル・リスタートをする機能をリスタート機能といいます。また，グレースフル・リスタートを補助する隣接装置をヘルパールータといいます。ヘルパールータにあるグレースフル・リスタートを補助する機能をヘルパー機能といいます。

SB-7800S では，リスタート機能とヘルパー機能をサポートしています。

SB-5400S では，ヘルパー機能だけをサポートしています。

以下に，IS-IS でグレースフル・リスタート機能を使用するときの構成上の条件を示します。以下の条件を満たさない場合，グレースフル・リスタートに失敗したり，グレースフル・リスタートが終了するまで通信できない経路ができたりすることがあります。

- グレースフル・リスタートするルータに，リスタート機能を設定してください。本装置でリスタート機能を設定する場合，コンフィグレーションコマンド options で graceful-restart パラメータを設定し，コンフィグレーションコマンド isis の graceful-restart サブコマンドで mode restart または mode both を設定してください。
- グレースフル・リスタートするルータの隣接ルータすべてに，ヘルパー機能を設定してください。本装置でヘルパー機能を設定する場合，コンフィグレーションコマンド isis の graceful-restart サブコマンドで mode helper または mode both を設定してください。

本装置では，グレースフル・リスタート情報の送信フィールドフォーマットを，RFC 3847 準拠と draft-ietf-isis-restart-03.txt 準拠から選択できます。本装置の IS-IS 隣接ルータの中に draft-ietf-isis-restart-03.txt またはそれ以前の規格に準拠した装置が 1 台でもある場合には，コンフィグレーションで準拠フォーマットを draft と指定してください。これは，RFC 3847 と draft-ietf-isis-restart-03.txt またはそれ以前の規格の間でフォーマットが異なるためです。RFC 3847 準拠装置は draft-ietf-isis-restart-03.txt に準拠したパケットを受信できますが，draft-ietf-isis-restart-03.txt 以前のドラフトに準拠した装置の中には，RFC 3847 準拠パケットを受信できないものがあります。

本装置は，RFC 3847 準拠フォーマット，draft-ietf-isis-restart-03.txt 以前のドラフトに準拠したフォーマットのどちらも受信可能です。

(2) リスタート機能【SB-7800S】

(a) リスタート機能の動作契機

以下に，本装置で IS-IS のリスタート機能が動作する契機を示します。

- BCU が系切替したとき。
- ルーティングプログラムが再起動したとき。

(b) グレースフル・リスタートの手順

次の図と表に IS-IS のグレースフル・リスタート手順を示します。

IS-IS では，グレースフル・リスタート後，LSP 学習が完了するまで，経路計算をしません。これは，部分的な LSP から誤った経路を求め，これにより以前の経路を上書きすることを防ぐためです。

また，全プロトコルがグレースフル・リスタートの経路情報学習を終えるまで，経路情報を広告しません。これは，すべてのプロトコルが経路学習し終わるまではルーティングテーブルが完全ではないので，広告経路が不足していたり，誤っていたりする可能性があるためです。

図 14-11　IS-IS グレースフル・リスタート手順

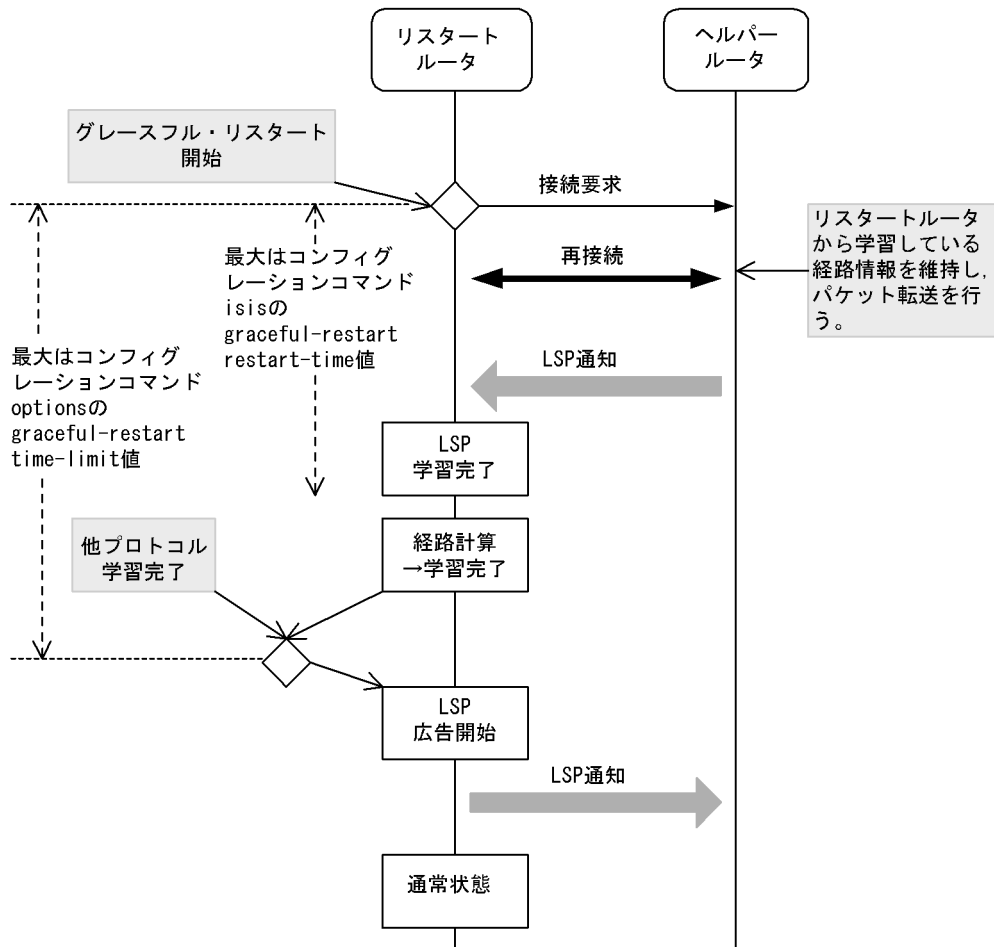



表 14-12 IS-IS グレースフル・リスタート手順

項番	項目	契機	処理内容
1	グレースフル・リスタートの開始	BCU が系切替したとき。	グレースフル・リスタートを開始します。隣接ルータと接続し，LSP を学習します。
		ルーティングプログラムが再起動したとき。	
2	経路計算	IS-IS インタフェースすべてについて，隣接ルータからすべての LSP を学習したとき。	経路計算して，ルーティングテーブルを更新します。この時点で，経路学習が完了します。この時点で LSP 学習が完了していない場合には IS-IS グレースフル・リスタート失敗とみなします。
3	広告開始	IS-IS の経路学習が完了し，かつ他のルーティングプロトコルの経路学習が完了したとき。	経路広告を開始します。広告完了後，通常の IS-IS 動作に戻ります。
		IS-IS のグレースフル・リスタートに失敗したとき。	

(c) グレースフル・リスタートが失敗するケース

以下に IS-IS のグレースフル・リスタートが失敗するケースを示します。

- グレースフル・リスタートの開始をヘルパールータへ通知してからコンフィグレーションコマンド isis の graceful-restart restart-time の時間が経過しても LSP 学習を完了できなかった場合。
- グレースフル・リスタートを開始してから経路保持時間 (コンフィグレーションコマンド options の graceful-restart time-limit の時間) が経過しても全プロトコルの経路学習が完了しなかった場合。
- コンフィグレーションコマンド isis の graceful-restart mode を変更し，リスタートルータ機能を削除した場合。
- コンフィグレーションコマンド options を変更し，グレースフル・リスタート機能を削除した場合。

なお，オーバロードビット機能を設定してある場合，グレースフル・リスタートに失敗すると，オーバロードビット機能が動作します。

(d) 注意事項

1. IS-IS のリスタート時間 (コンフィグレーションコマンド isis の graceful-restart restart-time の時間) を，系切替所要時間 + LSP 学習時間を超えるように設定してください。IS-IS が LSP を学習するためには，系切替が完了して IP インタフェースの Up/Down を確認できるようになっている必要があるからです。グレースフル・リスタート開始後，リスタート時間が経過した時点で LSP の学習が終わってない場合，IS-IS のグレースフル・リスタートに失敗します。
   系切替所要時間については，「12.8 グレースフル・リスタートの概要 表 12-30 系切替所要時間の目安値」を参照してください。
2. 本装置の系切替時ルーティングエントリ保持時間を，IS-IS のリスタート時間よりも長く設定してください。IS-IS のリスタート時間よりもルーティングエントリ保持時間のほうが短い場合，経路学習前に系切替前ルーティングエントリが削除されることがあります。
3. BGP4・BGP4+ のルーティングピアがグレースフル・リスタートを使用している場合，ルーティングピアのリスタート時間を IS-IS のリスタート時間よりも長く設定してください。
   ルーティングピアのリスタート時間のほうが短い場合，IS-IS が経路学習を完了する前にルーティングピアを接続することができず，ルーティングピアのグレースフル・リスタートに失敗することがあります。

（3） ヘルパー機能

本装置は，ヘルパー機能として，以下の機能をサポートします。

- グレースフル・リスタートをしたことを示すパケットを隣接ルータから受信したら，隣接ルータを切断せずに LSP 同期を開始します。

（a） ヘルパー機能の動作条件

コンフィグレーションでヘルパー機能の設定があれば特別な動作条件はありません。

（b） ヘルパー機能が失敗するケース

以下の場合，ヘルパー機能に失敗します。

- コンフィグレーションコマンド isis の graceful-restart mode を変更し，ヘルパー機能を削除した場合。

（c） 注意事項

1. 本装置の IS-IS 隣接ルータで IS-IS リスタート機能を使用する場合，本装置に IS-IS ヘルパー機能を設定してください。

14.2.9 高速経路切替機能

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報（第 1 優先経路と呼ぶ）と，第 1 優先経路の次に優先される経路（第 2 優先経路と呼ぶ）をあらかじめルーティングテーブルに登録しておき，インタフェースダウンによって第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディングテーブルに登録することで，通信停止時間の短縮を図る機能です。

IS-IS 単独で第 1 優先経路と第 2 優先経路の両方をルーティングテーブルに登録することはできませんが，スタティック経路など IS-IS 以外のプロトコルで生成した同一宛先の経路を組み合わせることによって，この機能を適用することが可能です（「表 13-7　高速経路切替を適用する経路の組み合わせ」または「表 18-7　高速経路切替を適用する経路の組み合わせ」を参照してください）。

高速経路切替機能の詳細については「13.2.5　高速経路切替機能」および「18.2.5　高速経路切替機能」を参照してください。

14.3 経路フィルタリング

経路フィルタリングには，入力経路を制御するインポート・フィルタと出力経路を制御するエキスポート・フィルタがあります。インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。エキスポート・フィルタは同一ルーティングプロトコル，またはルータ上で同時に動作している異なるプロトコルで学習した経路を広告するかどうかを制御します。

14.3.1 インポート・フィルタ (IS-IS)

インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。インポート・フィルタを指定していない場合は，すべての経路情報を取り込みます。

(1) プリファレンス値

取り込む経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，そのプロトコルのデフォルトのプリファレンス値になります。

同一宛先アドレスの経路情報が複数存在する場合，プリファレンス値によって優先度の高い経路情報が有効となります。プリファレンス値の詳細は，「14.2.4　経路学習」を参照ください

(2) フィルタリング条件

取り込む経路情報はフィルタリング条件で指定できます。指定できるインポート・フィルタのフィルタリング条件を次に示します。

- 学習元レベル
- 経路情報の経路種別
- 経路情報のメトリック種別
- 経路情報の宛先ネットワーク

14.3.2 エキスポート・フィルタ (IS-IS)

エキスポート機能はルータ上で同時に動作しているルーティングプロトコル間で経路情報を再配布します。つまり，学習元プロトコルで学習した経路情報を，配布先プロトコルを使用してそのほかのシステム (ルータ) に広告します。

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件 (送出先) と学習元プロトコルのフィルタリング条件 (送出経路情報) によって，特定の宛先に特定の経路情報を送出できます。また，配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値になります。

IS-IS では，配布先のレベルを指定することができます。また，付加情報としてメトリックとメトリック種別を指定できます。詳細は，「14.2.6　IS-IS 詳細　(3) 経路広告」を参照ください。なお，複数の配布先フィルタ条件を指定した場合，コンフィグレーションの定義順に検索して最初に一致したフィルタに従います。

なお，配布先プロトコルが，RIP または OSPFASE の場合は，「12.6.2　エキスポート・フィルタ (RIP/OSPF)」を参照してください。配布先プロトコルが，BGP4 の場合は，「13.4.2　エキスポート・フィルタ (BGP4)」を参照してください。配布先プロトコルが，RIPng，または OSPFv3 の場合は，「17.6.2　エキスポート・フィルタ (RIPng/OSPFv3)」を参照してください。配布先プロトコルが，BGP4+ の場合は，

「18.4.2　エキスポート・フィルタ (BGP4+)」を参照してください。

指定できる学習元のフィルタリング条件を次の表に示します。

表 14-13　学習元プロトコルのフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIP/RIPng	受信インタフェース 送信元ゲートウェイ 経路情報のタグ値 経路情報の宛先ネットワーク	RIP/RIPng で学習された経路情報
OSPF/OSPF6	OSPF ドメイン番号 経路情報の宛先ネットワーク	OSPF/OSPFv3 で学習された経路情報
OSPFASE/OSPF6ASE	OSPF ドメイン番号 経路情報のタグ値 経路情報の宛先ネットワーク	OSPF/OSPFv3 の AS 外経路情報
BGP4/BGP4+	送信元ピアアドレス 送信元 AS 番号 送信元ポリシーグループ番号 経路情報の AS_PATH 属性 経路情報の ORIGIN 属性 経路情報の Community 属性 経路情報の宛先ネットワーク	BGP4/BGP4+ で学習された経路情報
IS-IS	学習元レベル 経路情報の経路種別 経路情報のメトリック種別 経路情報の宛先ネットワーク	IS-IS で学習された経路情報
DIRECT	インタフェース 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	送出元インタフェース 経路情報の宛先ネットワーク	スタティックの経路情報
DEFAULT	経路情報の宛先ネットワーク	BGP4/BGP4+ の DEFAULT 経路情報
AGGREGATE	経路情報の宛先ネットワーク	経路集約によって生成された経路情報

14.4 経路集約 (IS-IS)

経路集約は一つまたは複数の経路情報から，該当する経路情報を包含するネットワークマスクのより短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含する一つの経路情報を生成し，隣接ルータなどに集約経路を通知して，ネットワーク上の経路情報の数を少なくする方法です。例えば，172.16.178.0/24 の経路情報や 172.16.179.0/24 の経路情報を学習した場合に，172.16.0.0/16 の集約された経路情報を生成するなどです。

経路集約の指定は，IS-IS の広告経路集約コマンド，またはコンフィグレーションコマンド aggregate(経路集約) で明示的に指定する必要があります。IS-IS の広告経路集約コマンドは，IS-IS への経路再配布専用であり，集約した経路は，IS-IS 以外のプロトコルでの経路広告や学習には影響しません。

(1) IS-IS の広告経路集約コマンド

IS-IS へ再配布する経路を集約することができます。レベル間広告経路およびほかのプロトコルで学習した経路を集約して広告します。集約経路の詳細は，「14.2.6 IS-IS 詳細 (4) 広告経路集約 (サマリー)」を参照ください。なお，集約元の経路情報は，エキスポート・フィルタで指定した学習元のフィルタ条件によって特定されます。

(2) aggregate(経路集約) コマンド

集約元の経路情報はフィルタリング条件によって特定できます。コンフィグレーションコマンド aggregate で指定できるフィルタリング条件を次の表に示します。

表 14-14 集約元経路情報のフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIP/RIPng	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIP/RIPng で学習された経路情報
OSPF/OSPF6	• 経路情報の宛先ネットワーク	OSPF/OSPFv3 で学習された経路情報
OSPFASE/OSPF6ASE	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPF/OSPFv3 の AS 外経路情報
BGP4/BGP4+	• 送信元 AS 番号 • 経路情報の AS_PATH 属性 • 経路情報の ORIGIN 属性 • 経路情報の宛先ネットワーク	BGP4/BGP4+ で学習された経路情報
IS-IS	• 学習元レベル • 経路情報の経路種別 • 経路情報のメトリック種別 • 経路情報の宛先ネットワーク	IS-IS で学習された経路情報
DIRECT	• 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 経路情報の宛先ネットワーク	スタティックの経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

また，集約元経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，集約経路のデフォルトのプリファレンス値 (130) が使用されます。なお，集約元の経路情報が学習されていない場合には集約経路情報は生成されません。

14.5　制限事項

なし。

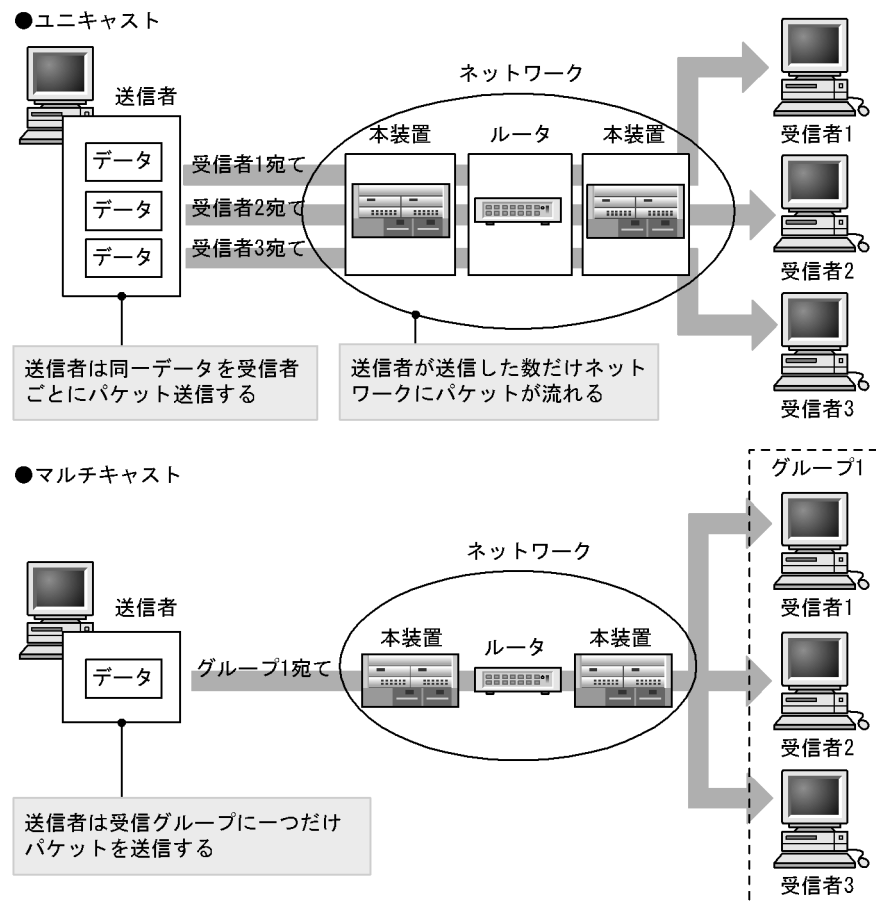
15 IPv4 マルチキャスト【OP-MLT】

マルチキャストは，ネットワーク内で選択されたグループに対して同一の情報を送信します。この章では IPv4 ネットワークで実現する IPv4 マルチキャストについて説明します。

15.1 IPv4 マルチキャスト概説

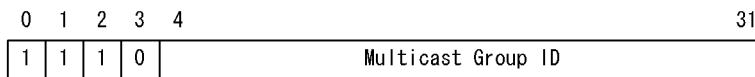
同一の情報を複数のユニキャストで送信すると，送信者とネットワークの負荷が大きくなります。マルチキャストでは，ネットワーク内で選択されたグループに対して同一の情報を送信します。マルチキャストは送信者が受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷が軽減します。

マルチキャストの概要を次の図に示します。

図 15-1　マルチキャストの概要 (IPv4)

15.1.1 IPv4 マルチキャストアドレス

マルチキャスト通信では IP アドレスの ClassD を使用します。マルチキャストアドレスはマルチキャストデータの送受信に参加しているグループの間だけで存在し，論理的なグループアドレスです。アドレスの範囲は 224.0.0.0 から 239.255.255.255 です。ただし 224.0.0.0 から 224.0.0.255 は予約されたアドレスです。マルチキャストアドレスのフォーマットを次の図に示します。

図 15-2　マルチキャストアドレスフォーマット

0	1	2	3	4　　　　　　　　　　　　　　　　31
1	1	1	0	Multicast Group ID

15.1.2　IPv4 マルチキャストのインタフェース種別

本装置でマルチキャストが動作できるインタフェース種別を次の表に示します。

表 15-1　マルチキャストのインタフェース種別

インタフェース種別			サポート	備考
LAN	イーサネット	マルチホーム未使用時	○	Ethernet V2 フレームタイプだけサポートする
		マルチホーム使用時	×	-
	Tag-VLAN 連携		○	-
	リンクアグリゲーション		○	-
	VLAN		○	-
	Private VLAN		×	-
POS			○	-
共用アドレスインタフェース			×	-
RM イーサネット (SB-5400S ではリモートマネージメントポート)			×	-
RM シリアル接続			×	-
装置 IP アドレス			×	マルチキャスト中継はできないが，ランデブーポイント候補および BSR 候補アドレスとして使用する
ローカルループバックインタフェース			×	-
Null インタフェース			×	-
トンネルインタフェース			×	-

(凡例)　○ : サポートする　× : サポートしない　- : 該当しない

15.1.3　IPv4 マルチキャストルーティング機能

本装置は受信したマルチキャストパケットをマルチキャスト中継エントリに従って中継します。マルチキャストルーティング機能は大きく分けて次の三つの機能があります。

- マルチキャストグループマネージメント機能
  グループメンバーシップ情報の送受信を行いマルチキャストグループの存在を学習する機能です。本装置では IGMP(Internet Group Management Protocol) を使用します。
- 経路制御機能
  経路情報の送受信を行って中継経路を決定し，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。経路情報収集には PIM-SM(PIM-SSM を含む)，PIM-DM または DVMRP を使用します。
- 中継機能

マルチキャストパケットをマルチキャスト中継エントリに従って，ハードウェアおよびソフトウェアで中継する機能です。

15.2 IPv4 マルチキャストグループマネージメント機能

マルチキャストグループマネージメント機能とは，ルータ - ホスト間でのグループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバーの存在を学習する機能です。本装置ではマルチキャストグループマネージメント機能実現のための管理プロトコルとして IGMP をサポートしています。

IGMP はルータ - ホスト間で使用されるマルチキャストグループ管理プロトコルです。ルータからのマルチキャストグループの参加問い合わせとホストからのマルチキャストグループへの参加・離脱報告によって，ルータがホストのマルチキャストグループへの参加・離脱を認識してマルチキャストパケットの中継・遮断を行います。

IGMPv3 は IPv4 マルチキャストグループマネージメント機能を実現する IGMPv2 を拡張したプロトコルで，指定した送信元からのマルチキャストパケットだけを受信する送信元フィルタリング機能が導入されています。IPv4 マルチキャストグループへの参加・離脱報告時に送信元指定ができるため，IGMPv3 と PIM-SSM と組み合わせて使用することで，効率の良い IPv4 マルチキャスト中継が実現できます。ただし，IGMPv3 は PIM-SM，PIM-SSM 使用時にだけ動作できます。

本装置が送信する IGMPv2 メッセージのフォーマットおよび設定値は RFC2236 に従います。また，IGMPv3 メッセージのフォーマットおよび設定値は RFC3376 に従います。

15.2.1 IGMP メッセージサポート仕様

(1) IGMPv2 メッセージのサポート仕様

IGMPv2 メッセージのサポート仕様を次の表に示します。

表 15-2 IGMPv2 メッセージのサポート仕様

タイプ		意味	サポート	
			送信	受信
Membership Query		マルチキャストグループの参加問い合わせ	-	-
-	General Query	全グループ宛て	○	○
	Group-Specific Query	特定グループ宛て	○	○
Version2 Membership Report		加入しているマルチキャストグループの報告 (IGMPv2 対応)	×	○
Leave Group		マルチキャストグループからの離脱報告	×	○
Version1 Membership Report		加入しているマルチキャストグループの報告 (IGMPv1 対応)	×	○

(凡例) ○：サポートする　×：サポートしない　- : 該当しない

(2) IGMPv3 メッセージのサポート仕様

IGMPv3 はフィルタモードと送信元リストを指定することで，送信元フィルタリング機能を実現します。フィルタモードには次の二つのモードがあります。

- INCLUDE : 指定された送信元リストからのパケットだけを中継します
- EXCLUDE : 指定された送信元リスト以外からのパケットだけを中継します

IGMPv3 メッセージのサポート仕様を次の表に示します。

表 15-3 IGMPv3 メッセージのサポート仕様

タイプ		意味	サポート	
			送信	受信
Version 3 Multicast Membership Query	General Query	IPv4 マルチキャストグループの参加問い合わせ（全グループ宛て）	○	○
	Group-Specific Query	IPv4 マルチキャストグループの参加問い合わせ（特定グループ宛て）	○	○
	Group-and-Source-Specific Query	IPv4 マルチキャストグループの参加問い合わせ（特定の送信元およびグループ宛て）	○	○
Version 3 Multicast Membership Report	Current State Report	加入している IPv4 マルチキャストグループとフィルタモード報告	×	○
	State Change Report	加入している IPv4 マルチキャストグループとフィルタモードの更新報告	×	○

（凡例） ○：サポートする　×：サポートしない

フィルタモードおよび送信元リストはグループ加入後に変更できます。変更は，Report メッセージに含まれる Group Record で指定します。本装置がサポートする Group Record タイプを次の表に示します

表 15-4 Group Record タイプ

タイプ		意味	サポート
Current State Report	MODE_IS_INCLUDE	INCLUDE モードであることを示します。	○
	MODE_IS_EXCLUDE	EXCLUDE モードであることを示します。	○※
State Change Report	CHANGE_TO_INCLUDE_MODE	フィルタモードを INCLUDE に変更することを示します。	○
	CHANGE_TO_EXCLUDE_MODE	フィルタモードを EXCLUDE に変更することを示します。	○※
	ALLOW_NEW_SOURCES	データの受信を希望する送信元を追加することを示します。	○
	BLOCK_OLD_SOURCES	データの受信を希望する送信元を削除することを示します。	○

（凡例） ○：サポートする
注※ 送信元リストは無視します。

15.2.2 IGMP 動作

（1） IGMPv2 の動作

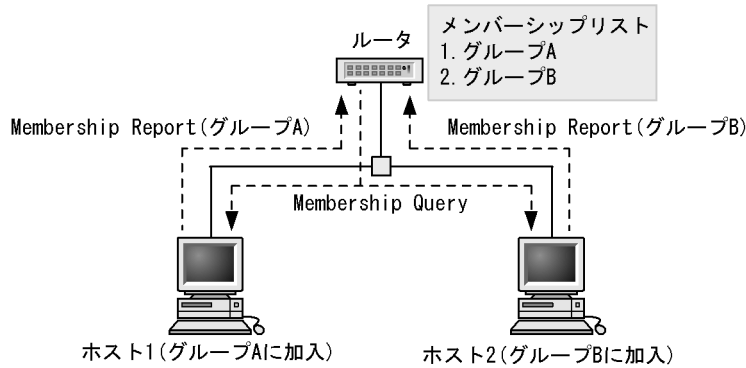
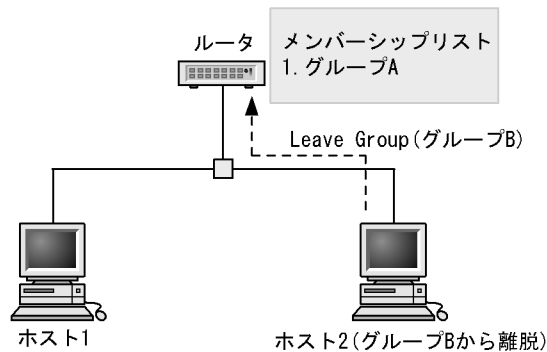
IGMPv2 メッセージを使用した IGMPv2 の動作を次に示します。

- IPv4 マルチキャストルータは，IPv4 マルチキャストメンバーシップの情報を得るため，定期的に直接接続するインタフェース上に Multicast Membership Query（General Query）メッセージを全マルチキャストホスト 224.0.0.1 宛てに送信します。

- ホストから Multicast Membership Report を受信すると，IPv4 マルチキャストルータはメンバーシップリストにそのグループを追加します。
- Multicast Leave Group メッセージを受信するとそのグループをメンバーシップリストから削除します。

IGMPv2 グループの参加・離脱を次の図に示します。

図 15-3 IGMPv2 グループの参加・離脱

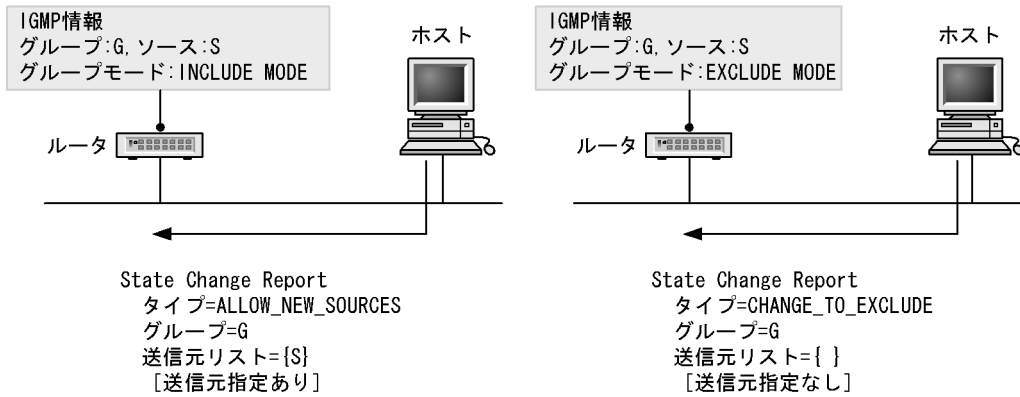
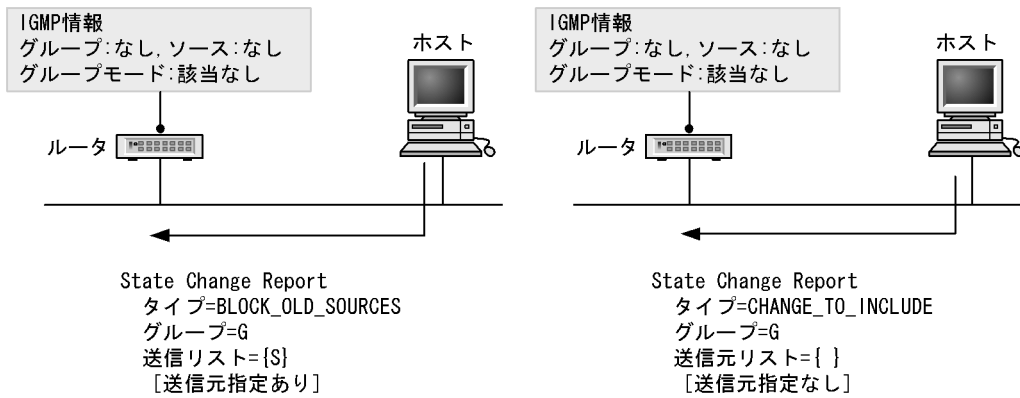
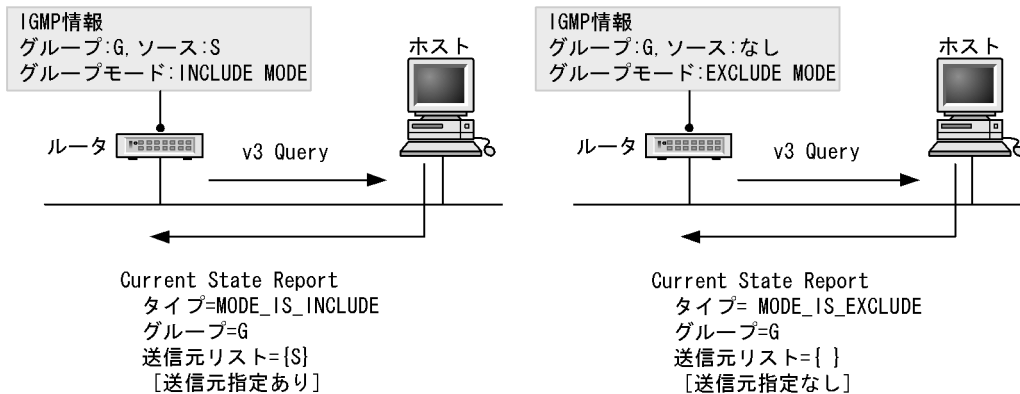
●ホスト1がグループA，ホスト2がグループBに加入する場合

●ホスト2がグループBから離脱する場合

(2) IGMPv3 の動作

IGMPv3 メッセージを使用した IGMPv3 の動作を次に示します。

- IPv4 マルチキャストルータは，IPv4 マルチキャストメンバーシップの情報を得るため，定期的に直接接続するインタフェース上に Version 3 Multicast Membership Query (General Query) メッセージを全マルチキャストホスト 224.0.0.1 宛てに送信します。
- ホストは Version 3 Multicast Membership Report（State Change Report および Current State Report）を 224.0.0.22 宛てに送信します。
- ホストから Version 3 Multicast Membership Report（State Change Report）メッセージを受信するとIPv4 マルチキャストルータは Group Record タイプの内容に応じてメンバーシップへのグループ追加，またはメンバーシップからのグループ削除を行います。
- ホストは Version 3 Multicast Membership Query を受信すると，グループへの参加状況を Version 3 Multicast Membership Report（Current State Report）で応答します。

ホストからの IGMPv3 Report メッセージ送信動作を次の図に示します。

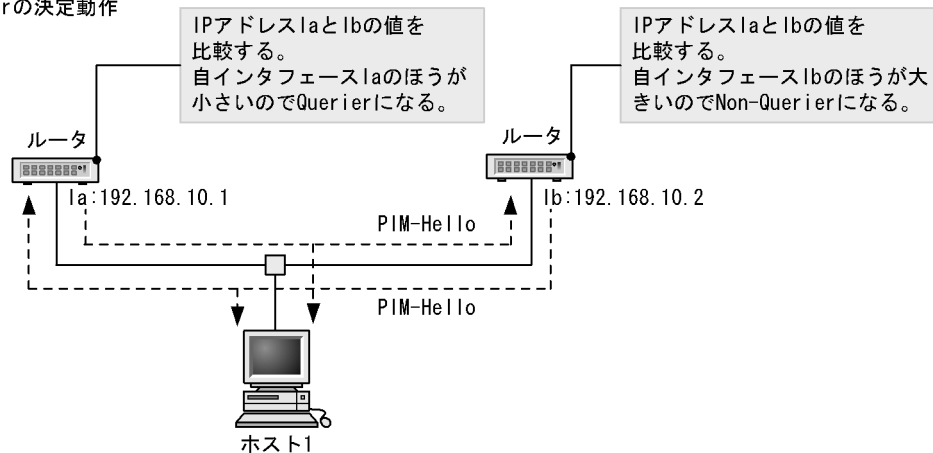
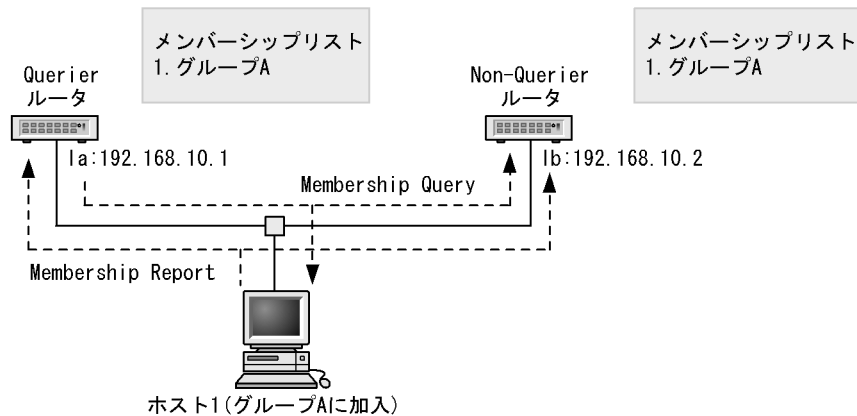
図 15-4　IGMPv3 グループの参加・離脱動作

●送信元Sを指定する場合と指定しない場合のグループGへの参加

●送信元Sを指定する場合と指定しない場合のグループGから離脱

●グループ参加時に送信元Sを指定した場合としない場合のQueryに対する応答

15.2.3　Querier の決定

（1）マルチキャストを PIM-DM で動作させた場合

IGMP ルータは Querier か Non-Querier のどちらか一方の役割を果たします。同一ネットワーク上に複数のルータが存在する場合，定期的な Membership Query メッセージを送信する Querier を決定します。

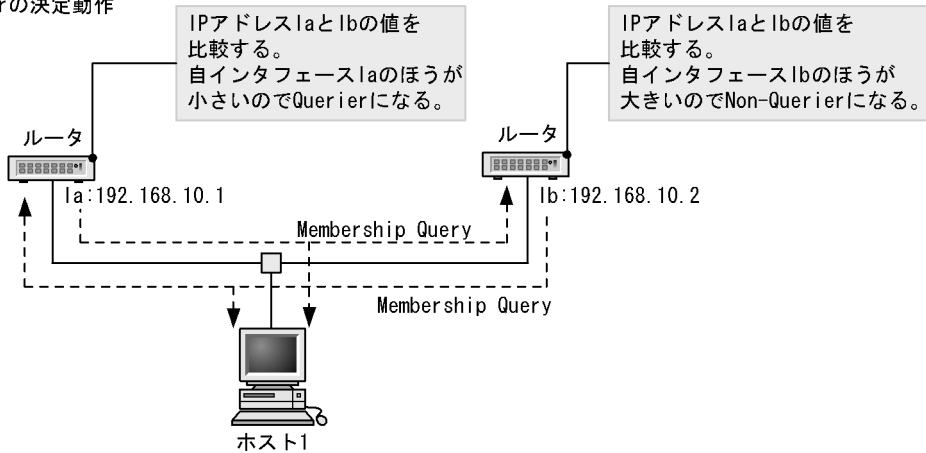
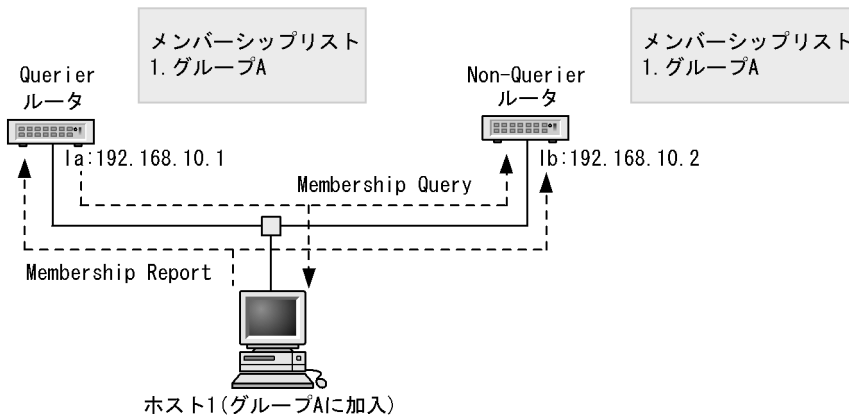
Querier の決定は，同一ネットワーク上に存在する PIM-DM ルータから受信した PIM-Hello の送信元 IP アドレスと自インタフェースの IP アドレスを比較し，自インタフェースの方が小さければ Querier として動作します。自インタフェースの方が大きければ Non-Querier となり Membership Query は送信しません。この動作によって同一ネットワーク上に Querier は一つだけ存在することになります。Querier と Non-Querier の決定を次の図に示します。

図 15-5　Querier と Non-Querier の決定 (マルチキャストを PIM-DM で動作させた場合)

Querier になった場合，送信元 IP アドレスが自インタフェースより小さい PIM-Hello を受信するまで Querier として動作し，Membership Query を 125 秒ごとに定期的に送信します。Non-Querier は Querier の PIM-Hello を受信することによって監視し，30 秒ごとに定期的に送信する PIM-Hello を一定時間 (デフォルト値は 105 秒) 受信しなかった場合に Querier として動作します。

(2)　マルチキャストを DVMRP および PIM-SM で動作させた場合

IGMP ルータは Querier か Non-Querier のどちらか一方の役割を果たします。同一ネットワーク上に複数のルータが存在する場合，定期的な Membership Query メッセージを送信する Querier を決定します。Querier の決定は，同一ネットワーク上に存在する IGMP ルータから受信した Membership Query の送信元 IP アドレスと自インタフェースの IP アドレスを比較し自インタフェースの方が小さければ Querier として動作します。自インタフェースの方が大きければ Non-Querier となり，Membership Query は送信しません。この動作によって同一ネットワーク上には Querier は一つだけ存在することになります。

Querier と Non-Querier の決定を次の図に示します。

図 15-6 Querier と Non-Querier の決定 (マルチキャストを DVMRP および PIM-SM で動作させた場合)

Querier になった場合，送信元 IP アドレスが自インタフェースより小さい Membership Query を受信するまで Querier として動作し，Membership Query を定期的 (デフォルト値 125 秒) に送信します。Non-Querier は Querier の Membership Query を受信することによって監視し，Membership Query 受信時 Membership Query の送信元 IP アドレスが自インタフェースよりも大きい場合，または Membership Query を一定時間 (デフォルト値 255 秒) 受信しなかった場合，Querier として動作します。

IGMPv3 ルータは IGMPv2 ルータと同じ方法で Querier を決定します。

15.2.4 グループメンバの管理

(1) IGMPv2 使用時の IPv4 グループメンバ管理

ホストからの Membership Report を受信することでグループメンバを登録します。また，Non-Querier でもホストからの Membership Report を受信することによって Querier 同様にグループメンバを登録します。

Querier が，ホストからあるグループへの離脱報告である Leave Group メッセージを受信した場合，離脱報告を受けたグループメンバに参加している他ホストの存在を確かめるため該当するグループ宛てに

Membership Query(Group-Specific Query) メッセージを連続して (1 秒間隔) 送信します。このメッセージを 2 回送信したあと，Membership Report を 1 秒間受信しない場合，該当するグループを削除します。また，Non-Querier の場合は Leave Group メッセージを無視します。

（2） IGMPv3 使用時の IPv4 グループメンバ管理

IGMPv3 使用時の IPv4 グループメンバの登録および削除について説明します。

ホストからマルチキャストグループへの加入要求を示す Report を受信することでグループ情報を登録します。ここでグループ情報とは，グループアドレスと該当するグループアドレスへの送信元アドレスを指します。Querier，Non-Querier と共に Report を受信することでグループ情報を登録します。

Querier は，マルチキャストグループからの離脱要求を示す Report を受信すると，該当するグループメンバに参加しているほかのホストの存在を確かめるため，送信元リストの指定有無に応じて次に示すメッセージを 1 秒間隔で送信します。

- 送信元リスト指定無し：Group-Specific Query メッセージ
- 送信元リスト指定有り：Group-and-Source-Specific Query メッセージ

本装置が Querier の場合は，上記のメッセージを 2 回送信後，1 秒間 Report を受信しなければ該当するグループ情報を削除します。本装置が Non-Querier の場合は，Querier が送信する上記メッセージを受信後，該当するグループ情報の削除処理を実行します。

15.2.5 IGMP タイマ

本装置が使用する IGMPv2 タイマ値を次の表に示します。タイマ Query Interval と Query Response Interval が変更できるのは DVMRP 使用時だけです。

表 15-5 IGMPv2 タイマ値

タイマ	内容	デフォルト値 (秒)	備考
Query Interval	Membership Query 送信周期時間	125	-※ 1，※ 2
Query Response Interval	Membership Report 最大応答待ち時間	10	-※ 1，※ 3
Other Querier Present Interval	Querier 監視時間	255	2 × Query Interval + Query Response Interval/2
Group Membership Interval	グループメンバの保持時間	260	2 × Query Interval + Query Response Interval
Startup Query Interval	Startup 時 General Query を送信する時間	30	-
Last Member Query Interval	離脱要求 受信後の Specific Query 送信周期	1	-

(凡例) - : 該当しない

注※ 1 DVMRP 使用時だけ変更できます。

注※ 2 「コンフィグレーションコマンドレファレンス Vol.1 igmp【OP-MLT】サブコマンド queryinterval」を参照してください。

注※ 3 「コンフィグレーションコマンドレファレンス Vol.1 igmp【OP-MLT】サブコマンド msbresptime」を参照してください。

本装置が使用する IGMPv3 タイマ値を次の表に示します。

表 15-6 IGMPv3 タイマ値

タイマ	内容	値（秒）	備考
Query Interval	Membership Query 送信周期時間	125	-
Query Response Interval	Multicast Membership Report 最大応答待ち時間	10	-
Other Querier Present Interval	Querier 監視時間	255	Robustness Variable × Query Interval + Query Response Interval/2 ※
Startup Query Interval	Startup 時 General Query を送信する時間	30	-
Last Member Query Interval	離脱要求 受信後の Specific Query 送信周期	1	-
Group Membership Interval	グループメンバの保持時間	260	Robustness Variable × Query Interval + Query Response Interval ※
Older Host Present Interval	IGMPv3 マルチキャストアドレス互換モードへの移行時間	260	Robustness Variable × Query Interval + Query Response Interval ※

（凡例） - : 特になし

注 IGMPv3 タイマ値は変更できません。

注※ Robustness Variable は本装置が Querier のとき 2，non-Querier のときは Querier の Robustness Variable に従います。

15.2.6 IGMPv1/IGMPv2/IGMPv3 装置との接続（PIM-SM，PIM-SSM 使用時）

本装置は IGMPv2 と IGMPv3 をサポートします。コンフィグレーションの multicast コマンドで，インタフェースごとに使用する IGMP バージョンを設定できます。指定するバージョンに応じた動作を次の表に示します。デフォルトは version 2 です。

表 15-7 IGMP バージョン指定時の動作

指定バージョン	バージョン指定時の動作
version 2	IGMPv2 で動作します。IGMPv3 パケットは無視します。
version 3	IGMPv2，IGMPv3 の両方で動作できます。IGMPv1，IGMPv2，IGMPv3 それぞれグループアドレス単位で動作します。
version 3 only	IGMPv3 で動作します。IGMPv1/v2 パケットは無視します。

（1） IGMPv2/IGMPv3 ルータとの接続

冗長構成などによって同一ネットワーク上に複数の IGMP ルータが存在する場合，互いの Query を受信することで Querier を決定します（「15.2.3 Querier の決定」を参照してください）。本装置は，IGMP バージョンが version 3 または version 3 only に設定されているインタフェースでの IGMPv2 ルータとの接続はサポートしません（v2 Query を無視するため，Querier を決定できなくなります）。IGMPv2 ルータと接続する場合は，該当するインタフェースの IGMP バージョンを version 2 に設定してください。

（2） IGMPv1/IGMPv2/IGMPv3 ホストとの接続

IGMPv1 ホスト，IGMPv2 ホストおよび IGMPv3 ホストが混在するネットワークと接続する場合は，該当するインタフェースの IGMP バージョンを version 3 に設定してください。ただし，IGMPv1 ホストと IGMPv2 ホストは IGMPv3 Query を受信できる（RFC 仕様）ことが必要になります。また，該当するインタフェースの IGMP バージョンを version 2 に設定した場合，IGMPv1 ホストと IGMPv2 ホストの混在をサポートします。IGMPv3 ホストは無視します。

IGMPv1 ホスト，IGMPv2 ホストおよび IGMPv3 ホストが混在する場合，グループメンバの登録はグループ加入を要求する IGMP のバージョンにより次の表に従います。

表 15-8　IGMPv1 ホストと IGMPv2 ホスト，IGMPv3 ホスト混在時のグループメンバ登録

グループ加入の要求	グループメンバの登録
IGMPv1 で受信	IGMPv1 モードでグループメンバを登録
IGMPv2 で受信	IGMPv2 モードでグループメンバを登録
IGMPv3 で受信	IGMPv3 モードでグループメンバを登録
IGMPv1 と IGMPv2 で受信	IGMPv1 モードでグループメンバを登録
IGMPv1 と IGMPv3 で受信	IGMPv1 モードでグループメンバを登録
IGMPv2 と IGMPv3 で受信	IGMPv2 モードでグループメンバを登録
IGMPv1 と IGMPv2 と IGMPv3 で受信	IGMPv1 モードでグループメンバを登録

15.2.7　静的グループ参加

IGMP 対応ホストが存在しないネットワークに IP マルチキャストパケットを中継するため，静的グループ参加機能を設定します。

静的グループ参加を設定したインタフェースは，Membership Report を受信しなくてもグループ参加したものと同様に動作します。

本機能は IGMPv2 の機能のため，該当するインタフェースの IGMP バージョンを version 3 only に設定している場合は動作しません。また，version 3 に設定されている場合は IGMPv2 でグループ参加したものと同様の動作をします。

15.2.8　IGMPv1 ルータとの混在

本装置は IGMPv2/IGMPv3 だけをサポートします。同一ネットワーク上に IGMPv1 ルータを混在させないでください。

15.2.9　IGMPv1 ホストとの混在（PIM-DM，DVMRP 使用時）

本装置は IGMPv1（RFC1112）ホストと IGMPv2（RFC2236）ホストの混在をサポートします。したがって，同一ネットワーク上に IGMPv1 ホストと IGMPv2 ホストが混在してもかまいません。

15.2.10　Querier の決定動作（PIM-DM 使用時）

本装置は PIM-DM 動作時，Querier の決定に PIM-Hello メッセージも使用するので同一ネットワーク上に複数のルータを接続する場合は必ずすべてのルータで PIM-DM を動作させてください。

15.2.11 IGMP 使用時の注意事項

- 構成変更によって静的グループ参加を設定した場合，PIM-SM グループの場合は (*,G) エントリ，PIM-SSM グループの場合は (S,G) エントリが作成されるまで最大 125 秒かかります。
- コンフィグレーションで設定している SSM アドレスの範囲外のグループに対して，送信元指定有りの IGMPv3 Report を受信した場合は，全送信元からのマルチキャストパケットを中継します。

15.2.12 適応ネットワーク構成

（1） 注意が必要な構成

次に示す構成で IGMP を使用する場合，注意が必要です。

● マルチキャストを 256 インタフェース以上で使用する場合，次の条件で使用してください。

- インタフェース当たりの参加グループ数は 2 までとする。
- 本装置が，Multicast Listener Report メッセージを 5 秒間に 600 以上受信しない。
（Multicast Listener Query（General Query）メッセージおよび Multicast Listener Query（Specific Query）メッセージに対する応答を含む※）

注※

本装置は，周期的に送信する Multicast Listener Query（General Query）メッセージを 5 秒間に最大 200 インタフェースまでとなるように調整しています。したがって，これに対する応答の Multicast Listener Report メッセージは 5 秒間に最大 400（条件である 600 以下）となります。

15.3　IPv4 マルチキャスト中継機能

マルチキャストパケットの中継処理はマルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで行います。一度中継したマルチキャストパケットの中継情報はハードウェアのマルチキャスト中継エントリに登録されます。マルチキャスト中継エントリに登録されたパケットはハードウェアで中継を行い，登録されていないパケットはソフトウェアのマルチキャスト経路情報から生成したマルチキャスト中継エントリに従って中継を行います。

(1) ハードウェアによるマルチキャストパケット中継処理

ハードウェアで行うマルチキャストパケット中継処理には次の機能があります。

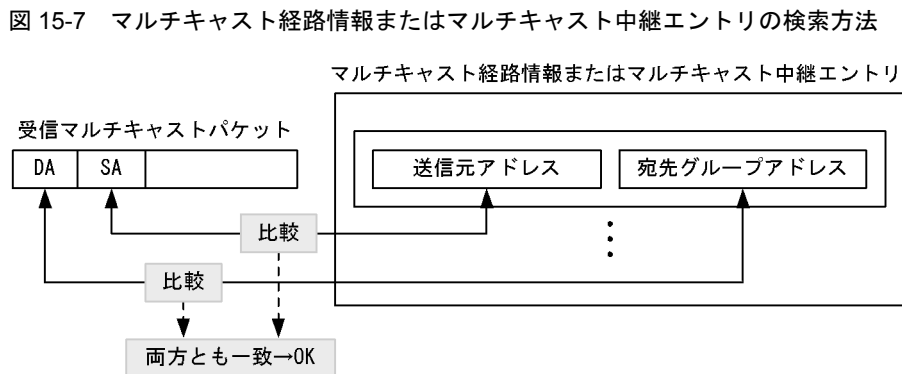
- マルチキャスト中継エントリの検索
  マルチキャストグループ宛てのパケットを受信した場合，ハードウェアのマルチキャスト中継エントリから該当エントリを検索します。
- マルチキャストパケットの受信インタフェースの正常性チェック
  マルチキャスト中継エントリの検索でエントリが存在した場合，そのパケットが正しいインタフェースから受信されているかどうかをチェックします。
- マルチキャストパケットのフィルタリング
  フィルタリングテーブルに登録された情報を参照して中継判断を行います。
- TTL に基づいた中継判断と TTL 値のデクリメント
  パケット中の TTL 情報から中継するかを判断し，中継する場合は該当パケットの TTL 値をデクリメントします。

(2) ソフトウェアによるマルチキャストパケット中継処理

- ハードウェアのマルチキャスト中継エントリにエントリが存在しない場合
  ある送信元からあるマルチキャストグループ宛てのパケットを最初に受信した場合，マルチキャスト経路情報から生成したマルチキャスト中継エントリに従って，ソフトウェアでパケットを中継します。同時に，ハードウェアに対して，マルチキャスト中継エントリを登録します。
- IP カプセル化処理を行う場合
  PIM-SM で一時的にランデブーポイント宛てに IP カプセル化を行い中継し，ランデブーポイントでは各中継先にカプセル化の解除を行い中継します。

(3) マルチキャスト経路情報またはマルチキャスト中継エントリの検索

受信したマルチキャストパケットの DA(宛先グループアドレス) と SA(送信元アドレス) に該当するエントリをマルチキャスト経路情報またはマルチキャスト中継エントリから検索します。マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法を次の図に示します。

図 15-7　マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法

（4） ネガティブキャッシュ

ネガティブキャッシュは，中継できないマルチキャストパケットをハードウェアによって廃棄する機能です。ネガティブキャッシュは中継先インタフェースの存在しない中継エントリです。ネガティブキャッシュは，中継できないマルチキャストパケットを受信すると，ハードウェアに登録します。その後，登録したマルチキャストパケットと同じアドレスのマルチキャストパケットを受信すると，そのパケットをハードウェアによって廃棄します。これによって，大量の中継できないマルチキャストパケットを受信しても，それを原因とする負荷上昇を抑えられます。

15.4 IPv4 経路制御機能

経路制御機能とは，マルチキャストルーティングプロトコルを使用して収集した隣接情報やグループ情報を基に，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。

15.4.1 IPv4 マルチキャストルーティングプロトコル概説

マルチキャストルーティングプロトコルは経路制御用のプロトコルです。本装置は次に示すマルチキャストルーティングプロトコルをサポートしています。

- PIM-SM(Protocol Independent Multicast-Sparse Mode)
  DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないで，マルチキャストの経路制御ができるプロトコルです。ランデブーポイントへのパケット送信後，最短パスで通信します。
- PIM-SSM(Protocol Independent Multicast-Source Specific Multicast)
  PIM-SSM は PIM-SM の拡張機能です。ランデブーポイントを使用しないで最短パスで通信します。
- PIM-DM(Protocol Independent Multicast-Dense Mode)
  DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないで，マルチキャストの経路制御ができるプロトコルです。パケットの送信後，不要な経路を除きます。
- DVMRP(Distance Vector Multicast Routing Protocol)
  距離ベクトル型の経路制御プロトコルです。

マルチキャストプロトコルの適応形態を次の表に示します。

表 15-9　マルチキャストルーティングプロトコルの適応形態

マルチキャストプロトコル	適応ネットワーク
PIM-SM	マルチキャストグループメンバーがまばらで散らばっているネットワーク
PIM-SSM	マルチキャストグループメンバーがまばらで散らばっているネットワーク
PIM-DM	マルチキャストグループメンバーが比較的集中しているネットワーク
DVMRP	マルチキャストグループメンバーが比較的集中しているネットワーク

なお，本装置で PIM-SM，PIM-DM，DVMRP の複数を同時に動作させることはできません。PIM-SSM は PIM-SM の拡張機能なので，PIM-SM と PIM-SSM は同時動作できます。コンフィグレーションでどれか一つのプロトコルを指定します。また，同一ネットワーク内に PIM-SM が動作しているルータ，PIM-DM が動作しているルータおよび DVMRP が動作しているルータが混在している場合，各ルータ間でマルチキャストパケットの中継は行われません。同一ネットワーク内でマルチキャストパケットの中継を行いたい場合は，すべてのルータで同じマルチキャストプロトコルが動作するように設定してください。各プロトコルの適応形態については，「15.6.3　適応ネットワーク構成」も参照ください。

15.4.2 IPv4 PIM-SM

PIM-SM はルータ間で使用されるマルチキャストルーティングプロトコルで，隣接情報やマルチキャスト配送ツリーへの参加および刈り込み要求などをやり取りすることによって，受信したマルチキャストパケットの中継および廃棄処理を実施します。PIM-SM は最初にランデブーポイント (集中ポイント) 経由でマルチキャストパケットを中継します。その後，既存のユニキャストルーティングを利用することによって，マルチキャストパケット送信元からの最短パスを使用して最短パス経由に切り替え，マルチキャストパケットを中継します。

本装置が送信する PIM-SM フレームのフォーマットおよび設定値は RFC2362 に従います。

(1) PIM-SM メッセージサポート仕様

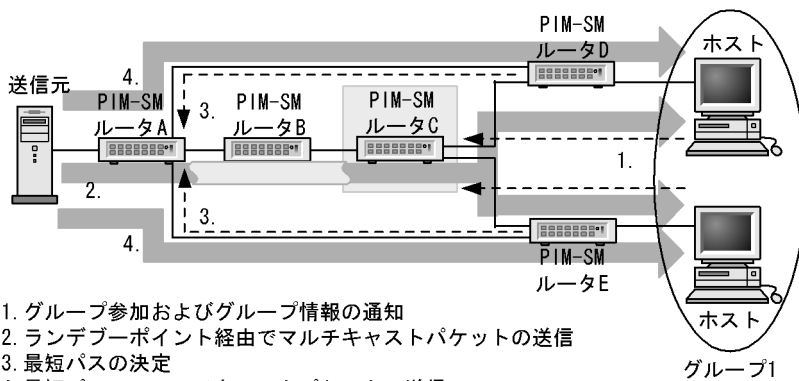
PIM-SM メッセージのサポート仕様を次の表に示します。

表 15-10 PIM-SM メッセージサポート仕様

メッセージタイプ	機能
PIM-Hello	PIM 近隣ルータの検出
PIM-Join ／ Prune	マルチキャスト配送ツリーの参加および刈り込み
PIM-Assert	Forwarder の決定
PIM-Register	マルチキャストパケットをランデブーポイント宛てに IP カプセル化する。
PIM-Register-stop	Register メッセージを抑止する。
PIM-Bootstrap	BSR を決定する。また，ランデブーポイントの情報を配信する。
PIM-Candidate-RP-Advertisement	ランデブーポイントが BSR に自ランデブーポイント情報を通知する。

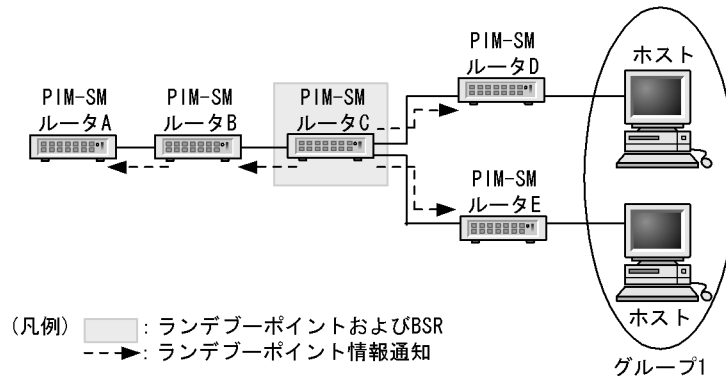
(2) 動作

各 PIM-SM ルータは IGMP で学習したグループ情報をランデブーポイントに通知します。ランデブーポイントは各 PIM-SM からグループ情報を受信することで各グループの存在を認識します。したがって，PIM-SM は最初にマルチキャストパケットをその送信元ネットワークからランデブーポイント経由ですべてのグループメンバに配送するために，送信元を頂点としたランデブーポイント経由配送ツリーを形成します。次に送信元から各グループに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信元からの最短パスを決定します（最短パス配送ツリーを形成します）。これによって送信元から各グループメンバへのマルチキャストパケット中継は最短パスで行われます。PIM-SM の動作概要を次の図に示します。

図 15-8 PIM-SM の動作概要

(a) ランデブーポイントおよびブートストラップルータ (BSR)

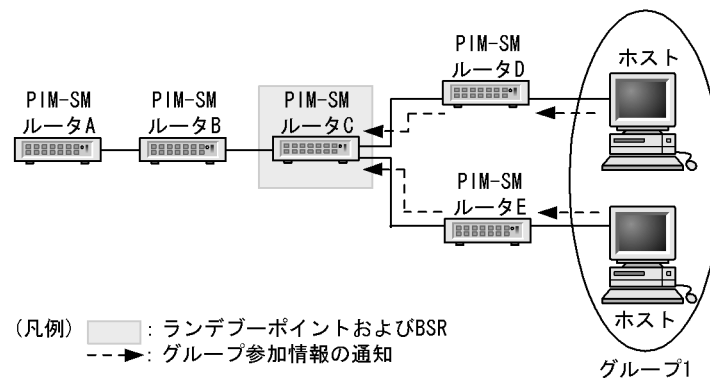
ランデブーポイントルータおよびブートストラップルータ (BSR) はコンフィグレーションで定義します。BSR はランデブーポイントの情報 (IP アドレスなど) をすべてのマルチキャストインタフェースに通知します。この通知はホップバイホップですべてのマルチキャストルータに通知されます。ランデブーポイン

トおよび BSR の役割を次の図に示します。

図 15-9　ランデブーポイントおよびブートストラップルータ (BSR) の役割

この図で，BSR(PIM-SM ルータ C) はランデブーポイント情報をすべてのマルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IP アドレスを学習し，受信したインタフェース以外でマルチキャストルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

(b)　ランデブーポイントへのグループ参加情報の通知

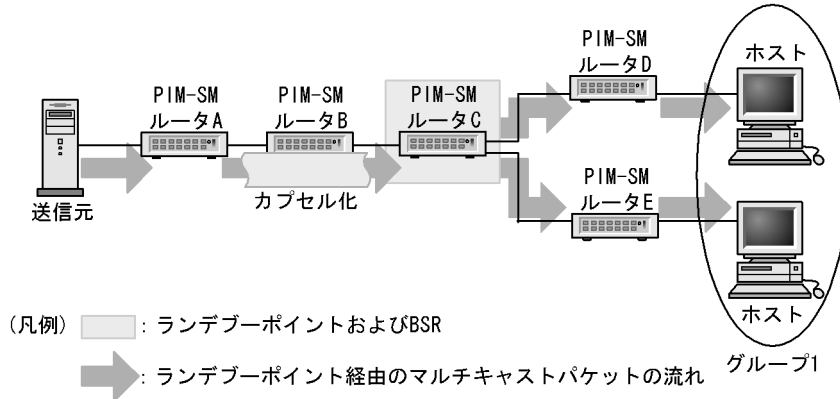
各ルータは IGMP で学習したグループ参加情報をランデブーポイントに通知します。ランデブーポイントはグループ情報を受信することでグループの存在をインタフェースごとに認識します。ランデブーポイントへのグループ参加情報の通知を次の図に示します。

図 15-10　ランデブーポイントへのグループ参加情報の通知

この図で，各ホストは IGMP でグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はグループ 1 情報を学習し，ランデブーポイント (PIM-SM ルータ C) にグループ 1 情報を通知します。ランデブーポイント (PIM-SM ルータ C) はグループ 1 情報を受信することによって，受信したインタフェースにグループ 1 が存在することを学習します。

(c)　ランデブーポイント経由のマルチキャストパケット通信 (カプセル化)

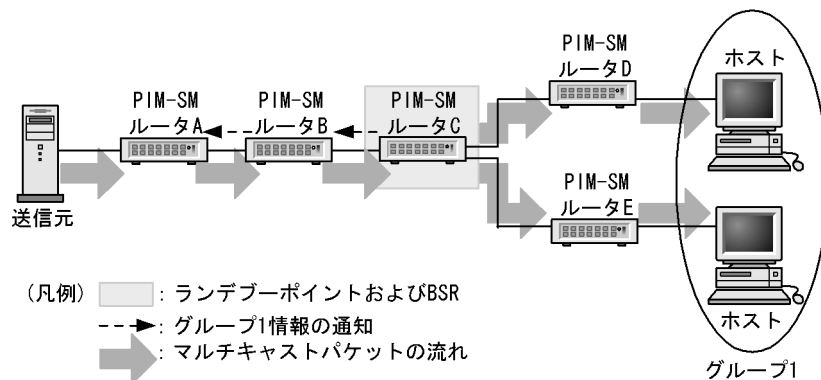
送信者 S1 がグループ 1 宛てのマルチキャストパケットを送信した場合，PIM-SM ルータ A はそのマルチキャストパケットをランデブーポイント (PIM-SM ルータ C) 宛てに IP カプセル化 (Register パケット) して送信します (ランデブーポイントの IP アドレスは (a) で学習済み)。ランデブーポイント (PIM-SM ルータ C) は IP カプセル化したパケットを受信すると，カプセル化を解除してグループ 1 が存在するインタフェースにグループ 1 宛てのマルチキャストパケットを中継します (グループ 1 の存在は (b) で学習済み

)。PIM-SM ルータ D および PIM-SM ルータ E は，グループ 1 宛てのマルチキャストパケットを受信すると，グループ 1 が存在するインタフェースにパケットを中継します (グループ 1 の存在は (b) の IGMP で学習済み)。ランデブーポイント経由のマルチキャストパケット通信 (カプセル化) を次の図に示します。

図 15-11　ランデブーポイント経由のマルチキャストパケット通信 (カプセル化)

(d)　ランデブーポイント経由のマルチキャストパケット通信 (非カプセル化)

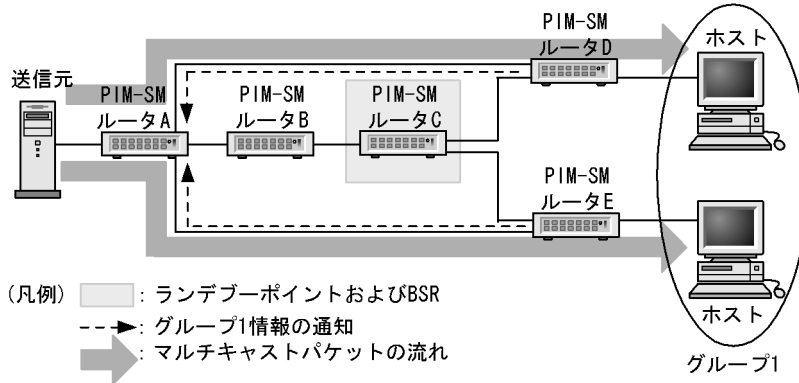
ランデブーポイント (PIM-SM ルータ C) は IP カプセル化したパケットを受信すると，カプセル化を解除してグループ 1 が存在するインタフェースにグループ 1 宛てのマルチキャストパケットを中継します。

ランデブーポイントはこの処理後，送信元サーバの方向にグループ 1 情報を通知します。グループ 1 情報を受信した PIM-SM ルータ B および PIM-SM ルータ A は受信したインタフェースにグループ 1 の存在を認識 (学習) します。PIM-SM ルータ A は送信元サーバが送信したグループ 1 宛てのマルチキャストパケットを IP カプセル化しないで該当するインタフェースに中継します。グループ 1 宛てのマルチキャストパケットを受信した PIM-SM ルータ B，PIM-SM ルータ C，PIM-SM ルータ D，PIM-SM ルータ E はグループ 1 が存在するインタフェースに中継します。ランデブーポイント経由のマルチキャストパケット通信 (非カプセル化) を次の図に示します。

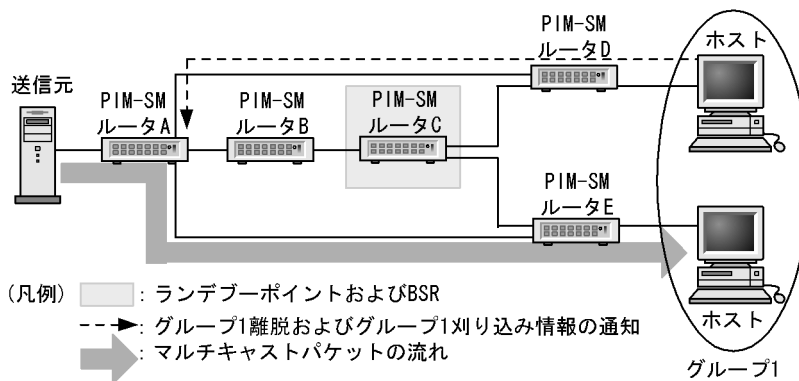
図 15-12　ランデブーポイント経由のマルチキャストパケット通信 (非カプセル化)

(e)　最短パスのマルチキャストパケット通信

PIM-SM ルータ D および PIM-SM ルータ E は，送信者元サーバのグループ 1 宛てマルチキャストパケットを受信した場合 ((c) で説明)，PIM-SM ルータ D および PIM-SM ルータ E は送信者 S1 に対して最短のパス (既存のユニキャストルーティング情報) の方向にグループ 1 情報を通知します。PIM-SM ルータ A は，PIM-SM ルータ D および PIM-SM ルータ E からグループ 1 情報を受信すると，受信したインタ

フェースにグループ 1 の存在を認識し，送信元サーバのグループ 1 宛てのマルチキャストパケットを受信すると該当するインタフェースに中継します。最短パスのマルチキャストパケット通信を次の図に示します。

図 15-13　最短パスのマルチキャストパケット通信

(f)　マルチキャスト配送ツリーの刈り込み

PIM-SM ルータ D は，ホストが IGMP でグループ 1 から離脱した場合，グループ 1 情報を通知していたインタフェースに対してグループ 1 の刈り込み情報を通知します。PIM-SM ルータ A はグループ 1 の刈り込み通知を受信すると，受信したインタフェースに対してグループ 1 宛てのマルチキャストパケットの中継を中止します。マルチキャスト配送ツリーの刈り込みを次の図に示します。

図 15-14　マルチキャスト配送ツリーの刈り込み

(3)　近隣検出

PIM-SM ルータはマルチキャストができるすべてのインタフェースに定期的に PIM-Hello メッセージを送信します。PIM-Hello メッセージは All-PIM-RoutersIP マルチキャストグループアドレス宛て (224.0.0.13) に送信します。このメッセージを受信することで，近隣の PIM ルータを動的に検出します。本装置は PIM-Hello メッセージの Generation ID オプションをサポートしています（RFC4601 および draft-ietf-pim-sm-bsr-07.txt に準拠)。Generaion ID はマルチキャストインタフェースごとに持つ 32 ビットの乱数で，PIM-Hello メッセージ送信時に Generation ID を付加して送信します。Generation ID はマルチキャストインタフェースが Up 状態になるたびに再生成します。受信した PIM-Hello メッセージに Generation ID オプションが付加されていれば Generation ID を記憶し，Generation ID の変化によって近隣装置のインタフェース障害を検出します。Generation ID の変化を検出すると，近隣装置情報の更新と PIM-Hello メッセージ，PIM Bootstrap メッセージおよび PIM Join/Prune メッセージを定期広告のタイミングを待たずに送信します。これによって，マルチキャスト経路情報を速やかに再学習できます。

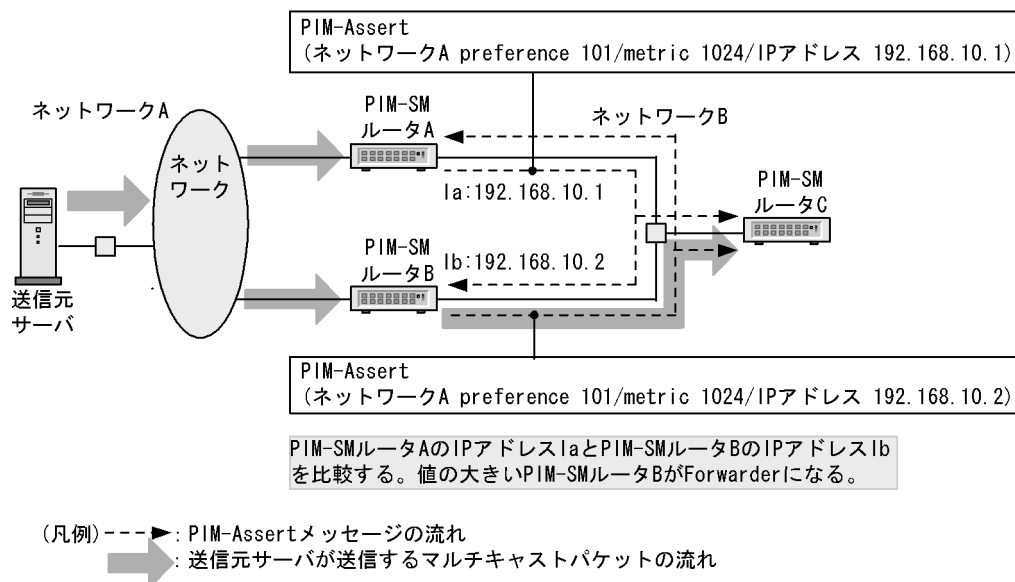
(4) Forwarder の決定

同一 LAN 上に複数の PIM-SM ルータが接続している場合，そのネットワークに重複パケットがフォワードされる可能性があります。PIM-SM ルータは同一 LAN 上に複数の PIM-SM ルータが存在した場合，PIM-Assert メッセージに含まれるメトリックを参照し，送信元ネットワークに対して最も小さいメトリックを持ったルータが同一 LAN 上にパケットをフォワードする権利を持ちます。もしメトリックが等しい場合，より大きい IP アドレスを持ったルータがフォワードする権利を持ちます。

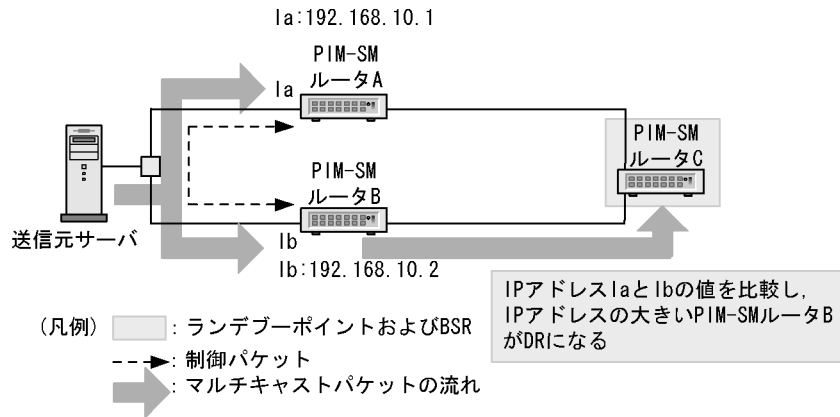
Forwarder を決定する流れを次に示します。

1. メトリックの preference を比較する。
2. preference が等しい場合に，メトリックを比較する。
3. 本装置は preference を 101，メトリックを 1024 固定で Assert メッセージを送信する。

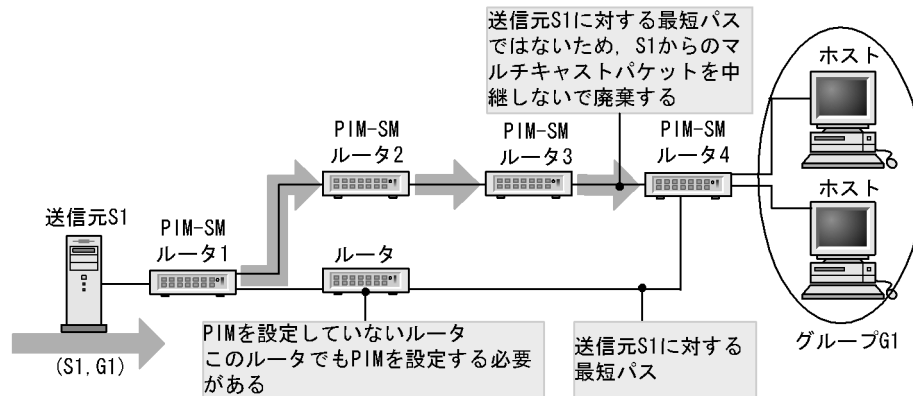
Forwarder の決定を次の図に示します。

図 15-15　Forwarder の決定

(5) DR の決定および動作

同一 LAN 上で複数の PIM-SM ルータが存在する場合，送信元サーバが送信したマルチキャストパケットをランデブーポイントに IP カプセル化して中継するルータ (DR) を決定します。そのインタフェース上で一番大きい IP アドレスのルータが DR となります。例えば，PIM-SM ルータ A と PIM-SM ルータ B の IP アドレスを比較して PIM-SM ルータ B の方が IP アドレスが大きい場合，PIM-SM ルータ B が DR となりランデブーポイントに対して IP カプセル化パケットを中継します。DR の動作を次の図に示します。

図 15-16　DR の動作

（6） 冗長経路時の注意事項

次の図に示すような冗長構成の場合，マルチキャストパケットがフォワードされないので注意してください。冗長経路がある場合は，その経路上のすべてのルータで PIM の設定が必要になります。

図 15-17　冗長経路時の注意

（7） PIM-SM タイマ仕様

PIM-SM が使用するタイマ値を次の表に示します。

表 15-11　PIM-SM タイマ

タイマ名	内容	デフォルト値（秒）	コンフィグレーションによる設定範囲（秒）	備考
Hello-Period	Hello の送信周期	30	10 ～ 3,600	-
Hello-Holdtime	隣接関係の保持期間	105	3.5 × Hello-Period	左記計算式より算出。
Assert-Timeout	Assert による中継抑止期間	180	-	-
Join/Prune-Period	Join/Prune の送信周期	60	30 ～ 3,600	最大で +50% の揺らぎが生じます。
Join/Prune-Holdtime	経路情報および中継先インタフェースの保持期間	210	3.5 × Join/Prune-Period	左記計算式より算出。

タイマ名	内容	デフォルト値(秒)	コンフィグレーションによる設定範囲(秒)	備考
Deletion-Delay-Time	Prune 受信後のマルチキャスト中継先インタフェースの保持期間	1/3 × 受信した Prune に含まれる保持期間	0 ～ 300	※ 1
Data-Timeout	中継エントリの保持期間	210	60 ～ 43, 200 または無期限	最大で +90 秒の誤差が発生します。
Register-Supression-Timer	カプセル化送信の抑止期間	60	-	最大で± 30 秒の揺らぎが生じます。
Probe-Time	カプセル化送信の再開確認を送信する時間	5	5 ～ 60	デフォルトの 5 秒では Register-Supression-Timer が満了する 5 秒前にカプセル化送信の再開確認 (Null-Register) を一度だけ送信します。※ 2
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60	-	-
RP-Holdtime	ランデブーポイント保持期間	150	2.5 × C-RP-Adv-Period	左記計算式より算出。
Bootstrap-Period	BSR メッセージ送信周期	60	-	-
Bootstrap-Timeout	BSR メッセージの保持期間	130	2 × Bootstrap-Period+ 10	左記計算式より算出。
BS_Rand_Override	BSR 切り替え遅延	5 ～ 23	-	-
Negative-Cache-Holdtime (PIM-SM)	ネガティブキャッシュの保持期間	210	10 ～ 3,600	PIM-SSM の場合は 3,600 秒の固定。

(凡例) - : 該当しない

注※ 1

本タイマ値はコンフィグレーションで設定された値が優先されるため，RFC2362 の規定とは異なった動作をします。ただし，コンフィグレーションで値を指定していない場合には RFC2362 の動作に準じます。

注※ 2

本タイマ値を 10 以上に設定すると，カプセル化送信の再開確認を 5 秒おきに複数回送信します。コンフィグレーションで値を指定していない場合には，一度だけ送信します。

(8) PIM-SM 使用上の注意事項

PIM-SM を使用したネットワークを構成する場合には次の制限事項に注意してください。本装置は RFC2362(PIM-SM 仕様) に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 15-12 RFC との差分

	RFC	本装置
パケット フォーマット	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにマスク長を設定するフィールドがある。	本装置ではエンコードアドレスのマスク長は 32 固定。
	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにアドレスファミリーとエンコードタイプを設定するフィールドがある。	本装置ではエンコードアドレスのアドレスファミリーは 1(IPv4)，エンコードタイプは 0 固定。 IPv4 以外の PIM-SM と接続できない。
	RFC には PIM メッセージのヘッダに PIM バージョンを設定するフィールドがある。	本装置の PIM バージョンは 2 固定。 PIM バージョン 1 と接続できない。
Join/Prune フラグメント	Join/Prune メッセージはネットワークの MTU を超えてもフラグメントすることができる。	本装置では送信する Join/Prune メッセージのサイズが大きい場合，8KB に分割して送信する。 さらに，分割して送信する Join/Prune メッセージはネットワークの MTU 長で IP フラグメントによって送信される。
PMBR との接続	RFC では PMBR(PIM Border Router) との接続および (*，*，RP) エントリについての仕様が記述されている。	本装置では PMBR との接続をサポートしていない。また，(*，*，RP) エントリもサポートしていない。
最短経路への切り替え	最短経路への切り替えタイミングとしてデータレートを基に切り替える方法がある。	本装置では last-hop-router にて最初のデータを受信したら，データレートをチェックしないで最短経路へ切り替える。
C-RP-Adv 受信と Bootstrap 送信	Bootstrap メッセージは生成したメッセージ長が最大パケット長を超えた場合にフラグメントすることが許される。しかし，フラグメント発生を抑止するためにランデブーポイント候補の最大数を定義することを推奨する。	ランデブーポイントで定義できるグループプレフィックスは最大 128 個である。 本装置では送信する Bootstrap メッセージのサイズが大きい場合，ネットワークの MTU 長で IP フラグメントして送信される。

15.4.3 IPv4 PIM-SSM

PIM-SSM は PIM-SM の拡張機能です。PIM-SM と PIM-SSM は同時動作できます。PIM-SSM が使用するマルチキャストアドレスは IANA で割り当てられています。本装置では，コンフィグレーションで PIM-SSM が動作するマルチキャストアドレス (グループアドレス) のアドレス範囲を指定できます。指定したアドレス以外では PIM-SM が動作します。

PIM-SM はマルチキャストエントリ作成にマルチキャスト中継パケットが必要なのに対し，PIM-SSM はマルチキャスト経路情報 (PIM-Join) の交換でマルチキャスト中継エントリを作成し，該当エントリでマルチキャストパケットを中継します。また，PIM-SSM ではランデブーポイントおよびブートストラップルータは必要ありません。したがって，マルチキャストパケットを中継するときに，パケットのカプセル化およびカプセル化の解除がなくなり，効率の良いマルチキャスト中継が実現できます。PIM-SSM は IGMPv3（INCLUDE モード）のホストと接続している場合に動作します。また，本装置では IGMPv2 または IGMPv3（EXCLUDE モード）のホストから PIM-SSM を利用できるようにする手段を提供します。

（1） PIM-SSM メッセージサポート仕様

PIM-SM メッセージサポート仕様 (「15.4.2 IPv4 PIM-SM (1) PIM-SM メッセージサポート仕様」) と同じです。

（2） PIM-SSM を動作させる前提条件

本装置のコンフィグレーションで次に示す設定が必要です。

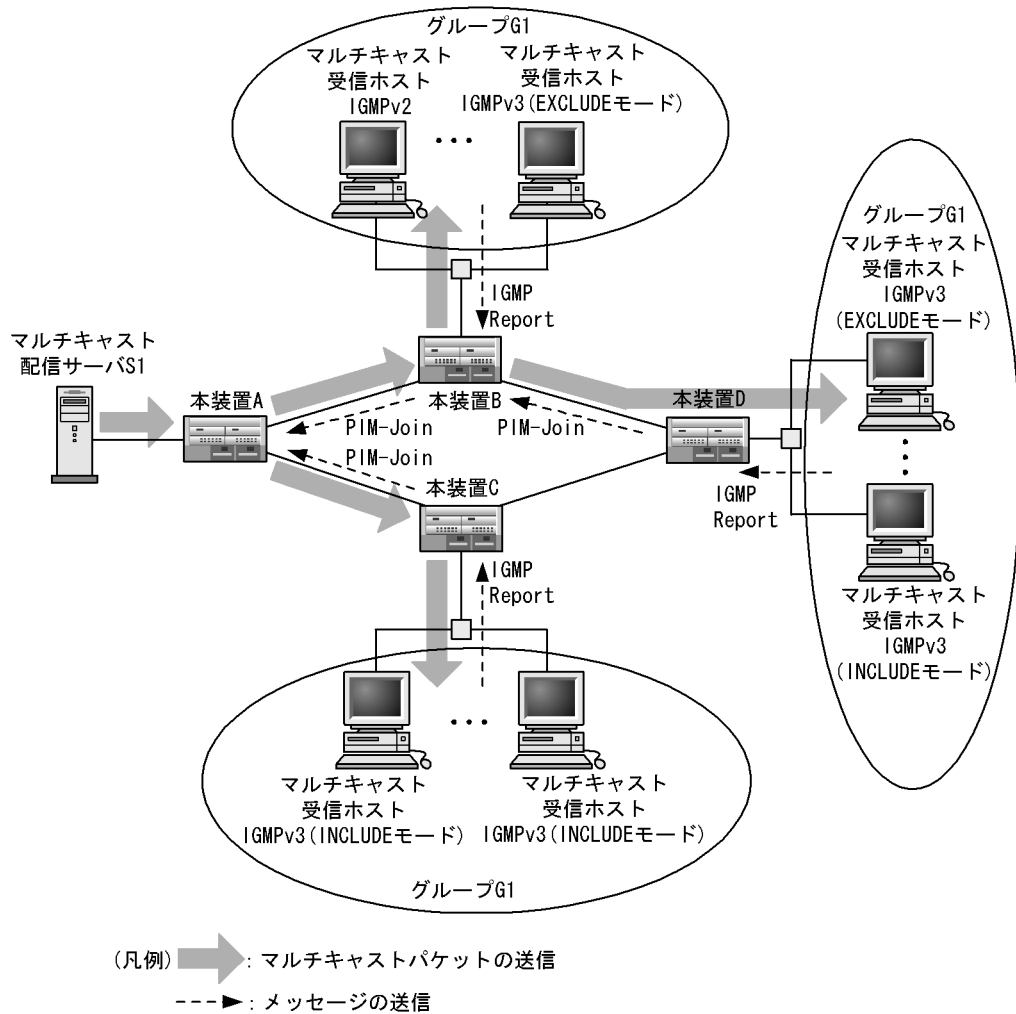
- 各装置の設定
  PIM-SSM が動作するグループアドレスの範囲を設定します。
- IGMPv3（INCLUDE モード）が動作するホストが直結している装置
  接続するインタフェースに IGMPv3 を設定します。
- IGMPv2 または IGMPv3（EXCLUDE モード）が動作するホストが直結している装置
  接続するインタフェースに IGMPv2 または IGMPv3 を設定します。
  使用するグループアドレスに送信元アドレスを設定します。

（3） PIM-SSM 動作（ホストが IGMPv3（INCLUDE モード）の場合）

マルチキャストパケット配信サーバ (送信元アドレス：S1) がグループ 1(グループアドレス：G1) にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（IGMPv3（INCLUDE モード））を受信します。
2. 参加要求（IGMPv3（INCLUDE モード））を受信した装置は通知されたグループアドレス (G1) と送信元アドレス (S1) から送信元アドレス (S1) の方向（ユニキャストのルーティング情報で決定）に PIM-Join を送信します。この場合，PIM-Join には，送信元アドレス (S1) とグループアドレス (G1) の情報が入ります。PIM-Join を受信した各装置は送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した装置は送信元アドレス (S1) とグループアドレス (G1) のマルチキャスト経路情報を学習します。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(G1) 宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってパケットを中継します。

PIM-SSM の動作概要を次の図に示します。

図 15-18　PIM-SSM の動作概要

(4) PIM-SSM 動作（ホストが IGMPv2 または IGMPv3（EXCLUDE モード）の場合）

マルチキャストパケット配信サーバ（送信元アドレス：S1）がグループ 1（グループアドレス：G1）にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（IGMPv2 または IGMPv3（EXCLUDE モード））を受信します。
2. 参加要求（IGMPv2 または IGMPv3（EXCLUDE モード））を受信した装置は通知されたグループアドレス (G1) とコンフィグレーションで設定したグループアドレスを比較します。グループアドレスが一致した場合，コンフィグレーションで設定した送信元アドレス (S1) の方向（ユニキャストのルーティング情報で決定）に PIM-Join を送信します。この場合，PIM-Join には，送信元アドレス (S1) とグループアドレス (G1) の情報が入ります。PIM-Join を受信した各装置は送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した装置は送信元アドレス (S1) とグループアドレス (G1) のマルチキャスト経路情報を学習します。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(G1) 宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってパケットを中継します。

PIM-SSM の動作概要については，「図 15-18　PIM-SSM の動作概要」を参照してください。

（5） 近隣検出

PIM-SM(「15.4.2 IPv4 PIM-SM （3）近隣検出」) と同じです。

（6） Forwarder の決定

PIM-SM(「15.4.2 IPv4 PIM-SM （4）Forwarder の決定」) と同じです。

（7） DR の決定および動作

PIM-SM(「15.4.2 IPv4 PIM-SM （5）DR の決定および動作」) と同じです。

（8） 冗長経路時の注意事項

PIM-SM(「15.4.2 IPv4 PIM-SM （6）冗長経路時の注意事項」) と同じです。

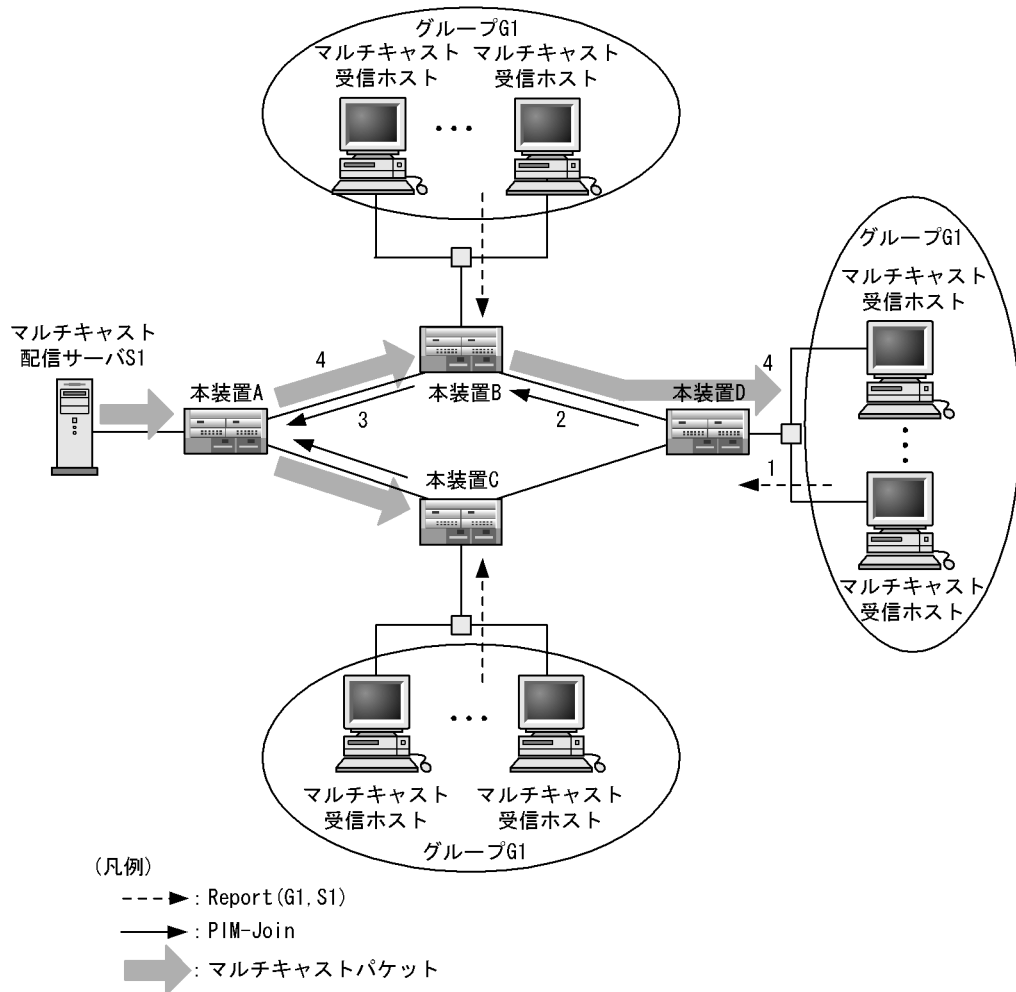
15.4.4 IGMPv3 使用時の IPv4 経路制御動作

（1） IGMPv3 使用時の IPv4 PIM-SSM 動作

PIM-SSM を使用するためには送信元の情報が必要となります。本装置では IGMPv2 を使用する際には送信元をコンフィグレーションで設定することで PIM-SSM を使用できます。IGMPv3 では送信元をコンフィグレーションで設定することなく PIM-SSM を使用できます（コンフィグレーションで PIM-SSM を設定する必要があります)。

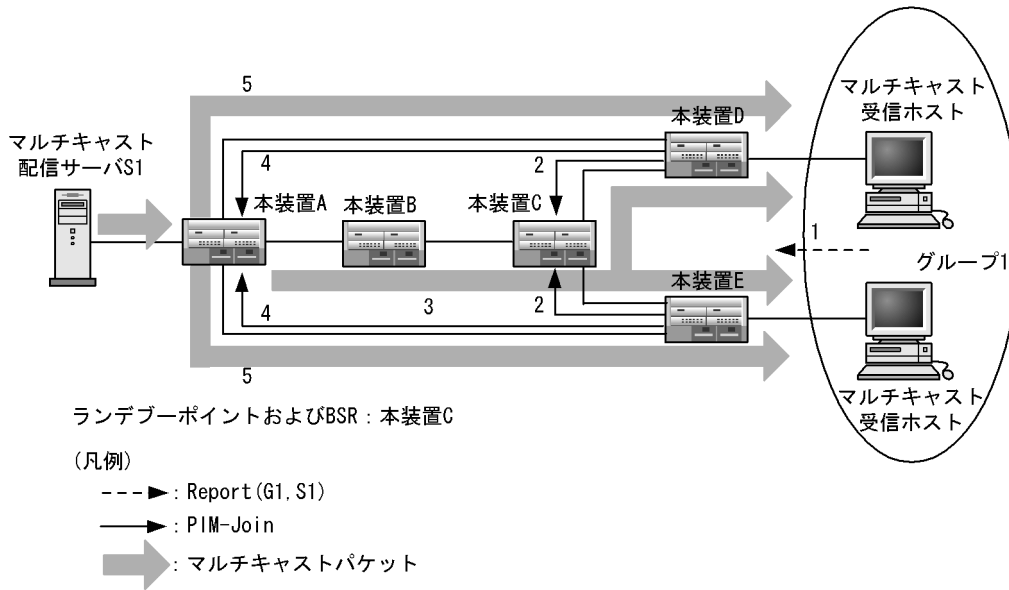
マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv4 PIM-SSM 動作を次に示します。

1. ホストからマルチキャストグループに参加するための IGMPv3 Report(G1,S1) を受信します。
2. IGMPv3 Report(G1,S1) を受信した装置は Report で通知されたグループアドレス (G1) とコンフィグレーションで定義したグループアドレスを比較します。グループアドレスが一致した場合は，Report で通知された送信元アドレス (S1) の方向にグループアドレス (G1) と送信元アドレス (S1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信した各装置は，送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した各装置は，PIM-Join を受信したインタフェースにだけ送信元アドレス S1 からのマルチキャストパケットを中継するように (S1,G1) の配送ツリーを形成します。
4. マルチキャスト配信サーバ S1 がグループ G1 宛に送信したマルチキャストパケットを受信した装置は，マルチキャスト中継情報に従ってマルチキャストパケットを中継します。

図 15-19　IGMPv3 使用時の IPv4 PIM-SSM 動作概要

(2) IGMPv3 使用時の IPv4 PIM-SM 動作

コンフィグレーションで PIM-SSM が設定されていない場合は PIM-SM で動作します。マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv4 PIM-SM 動作を次に示します。

1. ホストからマルチキャストグループに参加するための IGMPv3 Report(G1,S1) を受信します。
2. IGMPv3 Report(G1,S1) を受信した装置はランデブーポイントの方向にグループアドレス (G1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信したランデブーポイントは各グループの存在を認識します。マルチキャストパケットを送信元ネットワークからランデブーポイント経由で各グループメンバに配送するために，送信元を頂点としたランデブーポイント経由の配送ツリーを形成します。
4. 送信元から各グループメンバに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信元からの最短パスを決定します（PIM-Join を送信元の方向に送信し，最短パス配送ツリーを形成します)。
5. マルチキャスト配信サーバ S1 がグループ G1 宛に送信したマルチキャストパケットを受信した装置は，最短パス配送ツリーに従ってマルチキャストパケットを中継します。

図 15-20　IGMPv3 使用時の IPv4 PIM-SM 動作概要

（3） IGMPv1/IGMPv2 ホストおよび IGMPv3 ホスト混在時の IPv4 経路制御

IGMPv2 で PIM-SSM を使用する設定をしている状態で，IGMPv1/IGMPv2 ホストと IGMPv3 ホストが混在する場合の IPv4 経路制御動作について説明します。

コンフィグレーションで設定した PIM-SSM 対象アドレス範囲に含まれるグループアドレスに対して加入要求を受けた場合は PIM-SSM が動作します（表 15-13　IGMPv1/IGMPv2 および IGMPv3 ホスト混在時の IPv4 経路制御動作を参照）。IGMPv1/IGMPv2 Report で加入要求を受けた場合，送信元リストはコンフィグレーションで設定した送信元アドレスを使用します。IGMPv1/IGMPv2 Report と IGMPv3 Report で同じグループアドレスに対して加入要求を受けた場合，送信元リストはコンフィグレーションで設定された送信元アドレスと IGMPv3 Report に含まれる送信元リストを合わせたリストを使用します。

表 15-13　IGMPv1/IGMPv2 および IGMPv3 ホスト混在時の IPv4 経路制御動作

加入グループアドレス	IGMPv1 Report※1	IGMPv2 Report※2	IGMPv3 Report
SSM アドレス範囲内	PIM-SSM	PIM-SSM	PIM-SSM
SSM アドレス範囲外	PIM-SM	PIM-SM	PIM-SM

注※1　IGMPv1 ホストが送信する Report のグループアドレスに対してだけ IGMPv1 グループメンバを登録します。
注※2　IGMPv2 ホストが送信する Report のグループアドレスに対してだけ IGMPv2 グループメンバを登録します。

15.4.5　PIM-DM

PIM-DM はルータ間で使用されるマルチキャストルーティングプロトコルです。隣接情報やマルチキャスト配送ツリーへの参加および刈り込み要求などをやり取りし，受信したマルチキャストパケットの中継および廃棄処理を実施します。また，既存のユニキャストルーティングを利用することで，マルチキャストパケット送信元からの最短パスを使用してマルチキャストパケットを中継します。

本装置が送信する PIM-DM フレームのフォーマットおよび設定値は PIM-DM Internet-Draft に従います。

（1） PIM-DM メッセージサポート仕様

PIM-DM メッセージのサポート仕様を次の表に示します。

表 15-14　PIM-DM メッセージのサポート仕様

メッセージタイプ	機能
PIM-Hello	PIM 近隣ルータの検出
PIM-Join ／ Prune	マルチキャスト配送ツリーの参加および刈り込み
PIM-Assert	Forwarder の決定
PIM-Graft	マルチキャスト配送ツリーの再接続
PIM-Graft-Ack	PIM Graft メッセージに対する応答

（2） PIM-DM version1 との接続

本装置は，PIM-DM version2 だけをサポートしているため，version1 と接続できません。

（3） PIM-DM の動作

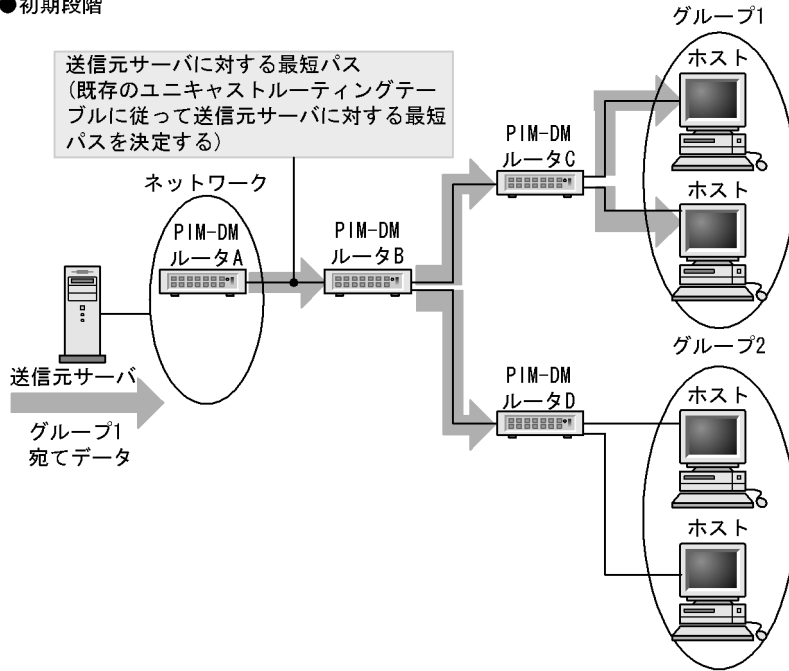
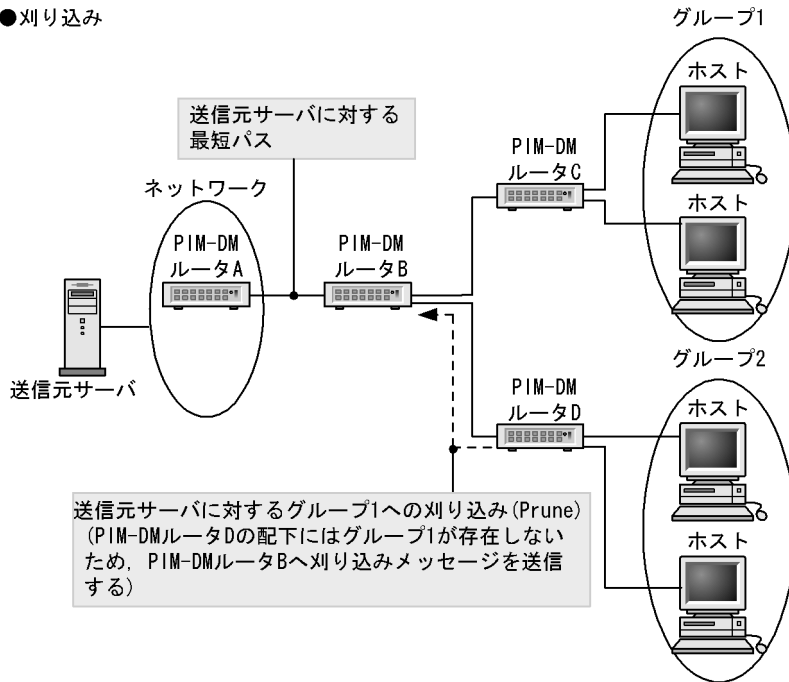
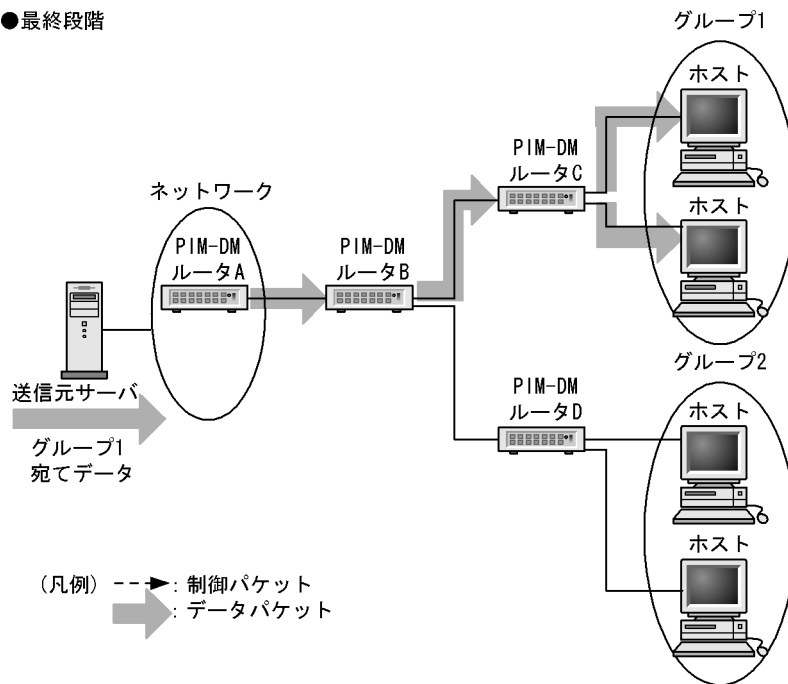
PIM-DM はマルチキャストパケットをその送信元ネットワークからすべてのグループメンバに配送するために，送信元を頂点とした配送ツリーを形成します。この配送ツリーはグループのすべてのメンバに到達するために必要な最小の配送ツリーに保持されます。グループメンバが存在しないインタフェースの場合，最初のマルチキャストパケット中継後に PIM-Prune で刈り込まれ，また，新しいメンバがグループに参加した場合，PIM-Graft メッセージの送受信によって，再度配送ツリーに付加されます。また，送信元から各グループに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信元からの最短パスを決定します。これは，受信したマルチキャストパケットを中継するときに，Reverse Path Forwarding チェックを行って送信元からの最短パス経由で受信したかどうかを判断するために使用します。

（a） 動作の流れ

PIM-DM は次に示す順序で動作します。

1. 最初のマルチキャストパケットを受信すると，マルチキャストが使用できるインタフェースすべてにパケットを中継します。
   マルチキャストパケットを受信した場合，マルチキャストが使用できるインタフェース (受信インタフェースは除く) すべてにパケットを中継します。
2. グループが存在しないインタフェースを刈り込みます。
3. 刈り込み動作終了後に，グループ 1 宛てのマルチキャストパケットを送信します。

この動作の流れを次の図に示します。

図 15-21 PIM-DM によるマルチキャストパケット中継処理

●最終段階

(4) 近隣検出

PIM-SM(「15.4.2　IPv4 PIM-SM　(3) 近隣検出」) と同じです。

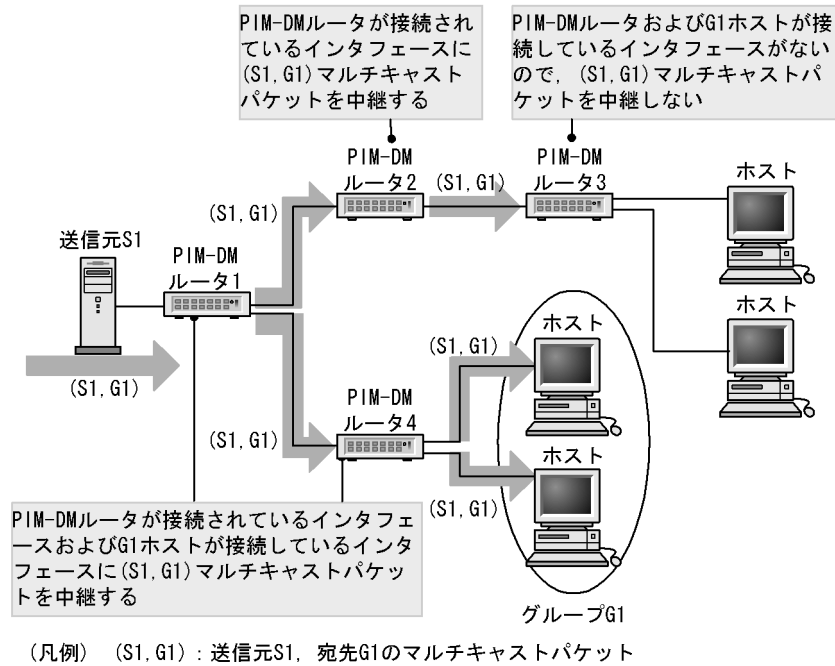
(5) Forwarder の決定

PIM-SM(「15.4.2　IPv4 PIM-SM　(4) Forwarder の決定」) と同じです。

(6) マルチキャスト配送ツリーの刈り込み

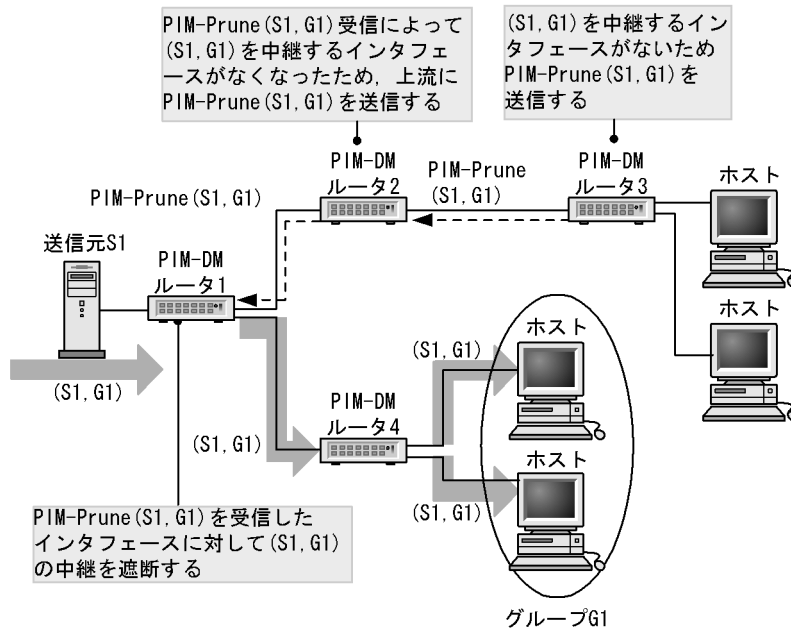
(a) 刈り込み前の動作

PIM-DM ルータは最初にマルチキャストパケットを受信したとき，中継できるインタフェース (PIM-DM 近隣ルータが存在する，または IGMP メンバーシップ情報があるインタフェース) のすべてを配送ツリーに登録します。中継できるインタフェースがない場合，送信元に対する次ホップルータ (Forwarder) に対して，中継する必要がないことを PIM-Prune(刈り込み) メッセージで通知します。PIM-Prune メッセージを受信した PIM-DM ルータは，あらかじめ登録してあった配送ツリーから PIM-Prune メッセージを受信したインタフェースを刈り込みます。マルチキャスト配送ツリーの刈り込み前の動作を次の図に示します。

図 15-22 マルチキャスト配送ツリー刈り込み前の動作

(b) 刈り込み動作

PIM-DM ルータ 3 では，(S1，G1) マルチキャストパケットを中継するインタフェースがないため (S1，G1) マルチキャストパケットを受信したインタフェースに対して PIM-Prune(S1，G1) を送信し，自ルータが該当するインタフェースから (S1，G1) マルチキャストパケットを受信する必要がないことを通知します。また，PIM-DM ルータ 2 は，PIM-Prune(S1，G1) を受信したことによって (S1，G1) マルチキャストパケットを中継するインタフェースがなくなったため (S1，G1) マルチキャストパケットを受信したインタフェースに対して PIM-Prune(S1，G1) を送信します。

マルチキャスト配送ツリーの刈り込み動作を次の図に示します。

図 15-23　マルチキャスト配送ツリーの刈り込み動作

（凡例）　PIM-Prune(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の刈り込み

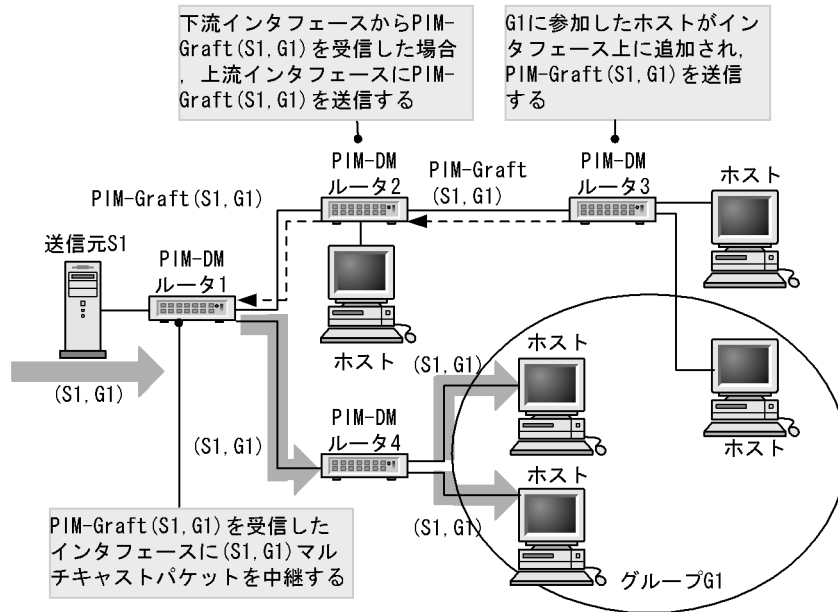
(7) マルチキャスト配送ツリーの再接続

マルチキャスト配送ツリーから刈り込んだツリーには該当する送信元から該当するグループへパケットは中継しません。しかし，刈り込んだツリーに新しくそのマルチキャストグループ参加があった場合，刈り込んだツリーに再接続 (PIM-Graft) メッセージを送信します。PIM-DM ルータは Graft メッセージを受信したら配送ツリーにそのインタフェースを追加し Graft Ack メッセージを返信します。

(a) 再接続動作

PIM-DM ルータ 3 で，新しく G1 に参加したホストが下流インタフェース上に追加された場合，G1 に対して PIM-Prune(S1，G1) を送信したインタフェースに PIM-Graft(S1，G1) を送信し再接続要求をします。PIM-DM ルータ 2 では，PIM-Prune(S1，G1) を受信したインタフェースから PIM-Graft(S1，G1) を受信した場合，PIM-Prune(S1，G1) を送信したインタフェースに PIM-Graft(S1，G1) を送信します。

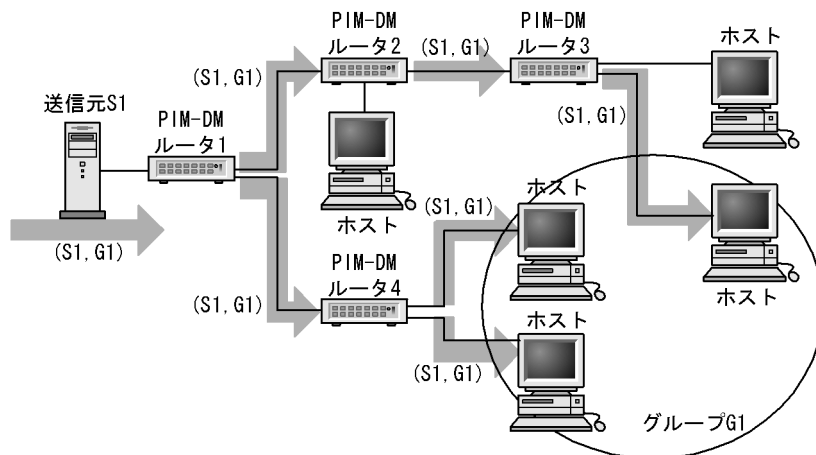
「図 15-23　マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から新しくそのマルチキャストグループに参加があった場合の，マルチキャスト配送ツリーへの再接続動作を次の図に示します。

図 15-24　マルチキャスト配送ツリーへの再接続動作

（凡例）　(S1,G1)：送信元S1，宛先G1のマルチキャストパケット
　　　　PIM-Graft(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の再接続

(b)　再接続後のマルチキャストパケットの流れ

PIM-DM ルータ 1 にはマルチキャストパケットが中継されているため，PIM-Graft(S1,G1) を受信したインタフェースに (S1,G1) マルチキャストパケットを中継します。

「図 15-23　マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から新しくそのマルチキャストグループに参加があった場合の，マルチキャスト配送ツリーへの再接続後動作を次の図に示します。

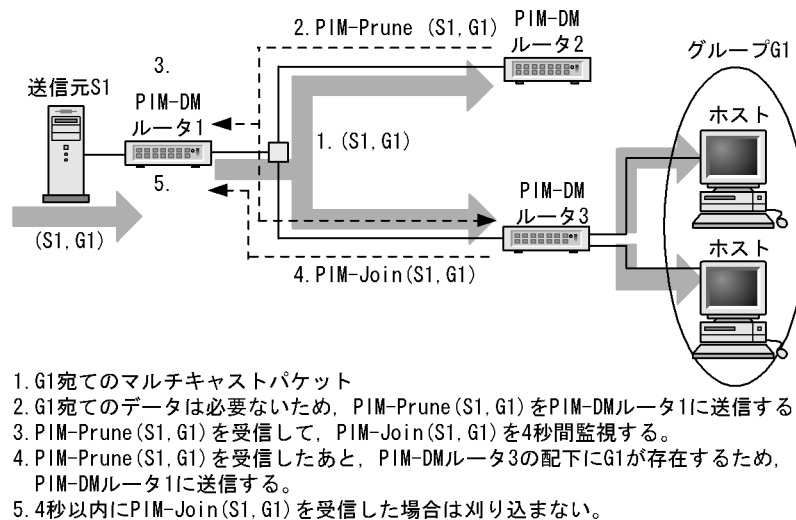
図 15-25　マルチキャスト配送ツリーへの再接続後動作

（凡例）　(S1,G1)：送信元S1，宛先G1のマルチキャストパケット

(8)　同一 LAN 上の刈り込み

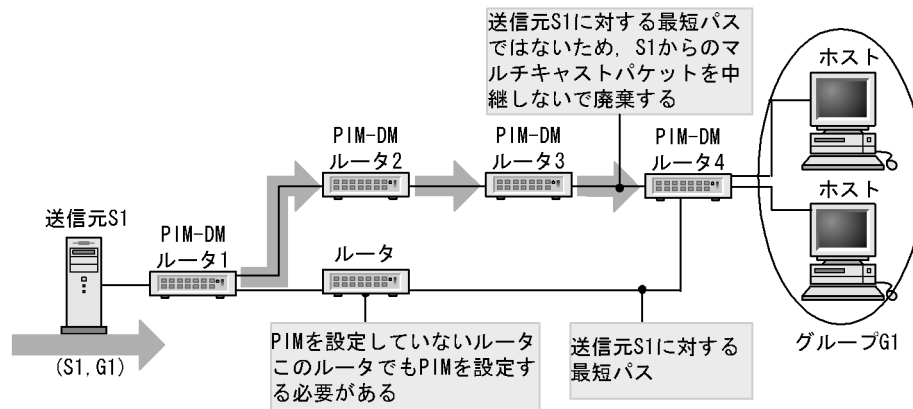
同一 LAN 上で PIM-DM ルータ 2 が PIM-DM ルータ 1 にグループ G1 に対しての PIM-Prune メッセージを送信した場合，PIM-DM ルータ 1 はそのインタフェースを刈り込むまで 4 秒間待ちます。その間にグ

ループ G1 の PIM-Join(以前に送信された PIM-Prune メッセージをキャンセルする) メッセージを受信しない場合は，そのインタフェースを刈り込みます。PIM-Join を受信した場合は，刈り込みを中止します。PIM-DM ルータ 3 は PIM-DM ルータ 2 が PIM-DM ルータ 1 に対して送信した PIM-Prune メッセージを受信して，もし自装置が PIM-DM ルータ 1 からグループ G1 宛てのパケットを受信したい場合は，3 秒以内に PIM-DM ルータ 1 に PIM-Join メッセージを送信し，PIM-DM ルータ 1 に刈り込みをキャンセルさせます。Multi-access LAN 上での PIM-Prune および PIM-Join の動作を，次の図に示します。

図 15-26　Multi-access LAN 上での PIM-Prune および PIM-Join の動作

1.G1宛てのマルチキャストパケット
2.G1宛てのデータは必要ないため，PIM-Prune(S1,G1)をPIM-DMルータ1に送信する。
3.PIM-Prune(S1,G1)を受信して，PIM-Join(S1,G1)を4秒間監視する。
4.PIM-Prune(S1,G1)を受信したあと，PIM-DMルータ3の配下にG1が存在するため，PIM-Join(S1,G1)をPIM-DMルータ1に送信する。
5.4秒以内にPIM-Join(S1,G1)を受信した場合は刈り込まない。

(9) 冗長経路時の注意事項

次の図に示すような冗長構成の場合，マルチキャストパケットがフォワードされないので注意してください。したがって，冗長経路がある場合は，その経路上のすべてのルータで PIM の設定が必要になります。

図 15-27　冗長経路時の注意

(10) PIM-DM タイマ仕様

PIM-DM が使用するタイマ値を次の表に示します。

表 15-15 PIM-DM タイマ

タイマ	値 (秒)	備考
PIM-Hello 周期	30	-
近隣タイムアウト	105	3.5 × PIM-Hello 周期
PIM-Assert タイムアウト	210	-
PIM-Prune Delay タイマ	4	-
Prune Life Time	210	PIM-Prune を受信している場合は，受信している PIM-Prune の Life time の最大値

(凡例) - : 該当しない
注 PIM-DM タイマの値は変更できない。

15.4.6 DVMRP

DVMRP はルータ間で使用されるマルチキャストプロトコルで，隣接情報やマルチキャスト配送ツリーへの参加および刈り込み要求などの送受信によって，マルチキャストパケットの中継および廃棄処理を実施します。DVMRP では経路情報を交換して得られたマルチキャスト経路情報から新しくマルチキャスト中継エントリを作成し，マルチキャストパケットを中継します。

本装置が送信する DVMRP フレームのフォーマットおよび設定値は DVMRP Internet-Draft に従います。

(1) DVMRP メッセージサポート仕様

DVMRP メッセージのサポート仕様を次の表に示します。

表 15-16 DVMRP メッセージのサポート仕様

メッセージタイプ	機能
DVMRP-Probe	DVMRP 近隣ルータの検出
DVMRP-Report	ユニキャスト経路情報の交換
DVMRP-Prune	マルチキャスト配送ツリーの刈り込み
DVMRP-Graft	マルチキャスト配送ツリーの再接続
DVMRP-Graft-Ack	DVMRP-Graft メッセージに対する応答

(2) DVMRP の動作

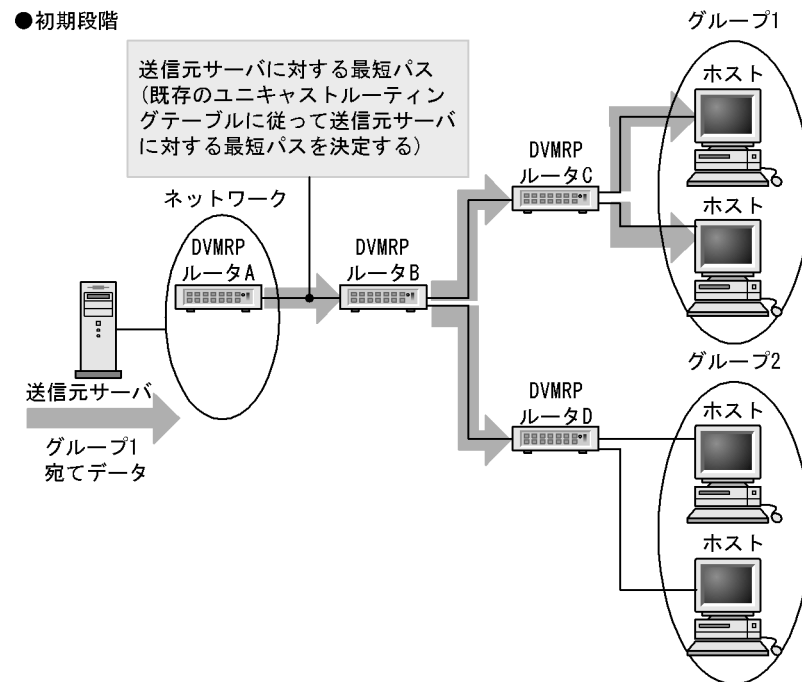
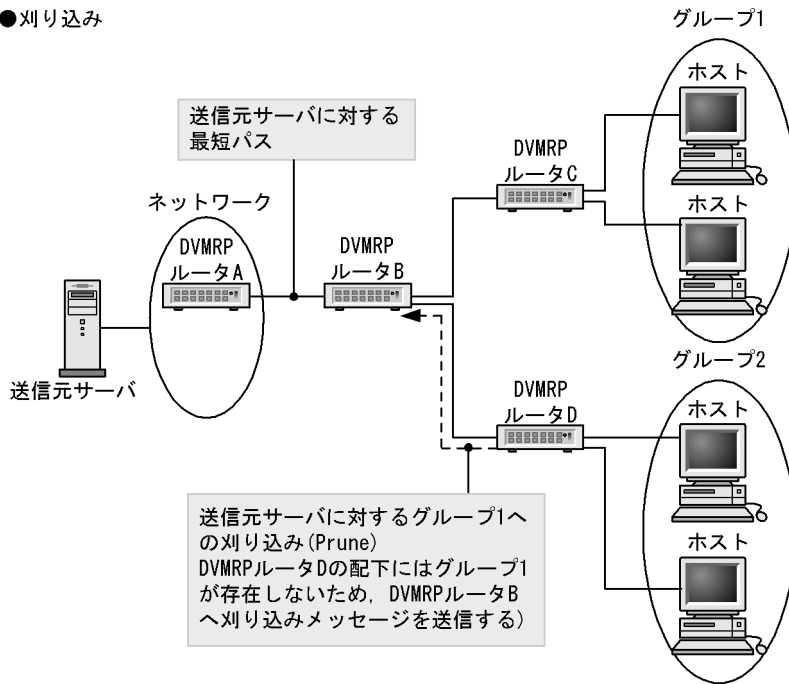
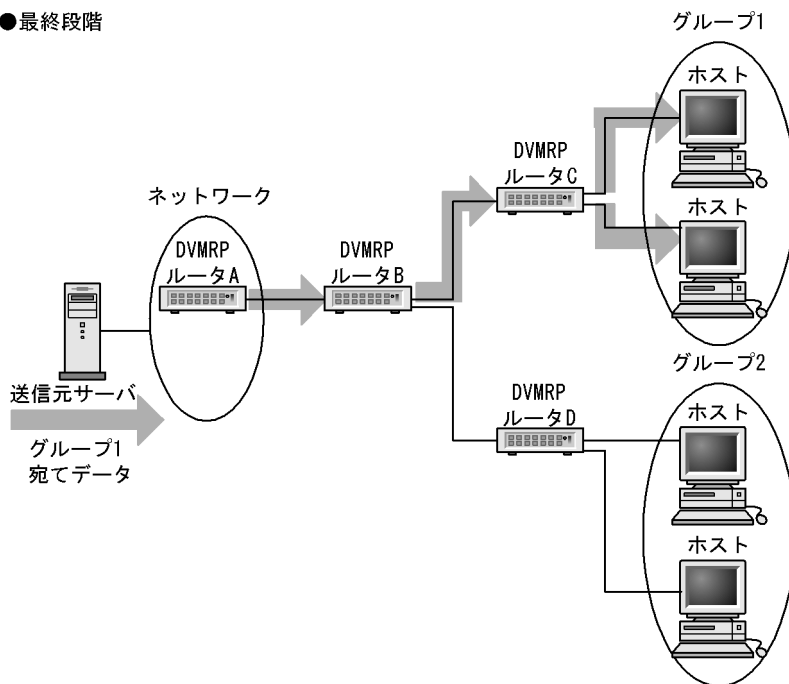
DVMRP はマルチキャストパケットを送信元ネットワークからすべてのグループメンバに配送するために，送信元を頂点とした配送ツリーを形成します。この配送ツリーはグループのすべてのメンバに到達するために必要な最小の配送ツリーに保たれます。まず，送信元から各グループに対して最短パスで到達できるように，距離ベクタルーティングアルゴリズムを使用して送信元からの最短パスを決定します。これは，受信したマルチキャストパケットを中継するとき，Reverse Path Forwarding チェックを行わない，送信元からの最短パス経由で受信したかの判断に使用します。グループメンバが存在しないインタフェースの場合，最初のマルチキャストパケット中継後 DVMRP-Prune で刈り込まれ，また，新しいメンバがグループに参加した場合，DVMRP-Graft メッセージの送受信によって再度配送ツリーに付加されます。

(a) 動作の流れ

DMMRP は次に示す順序で動作します。

1. 最初のマルチキャストパケットを受信すると，マルチキャストが使用できるインタフェースすべてにパケットを中継します。
   マルチキャストパケットを受信した場合，マルチキャストが使用できるインタフェース（受信インタフェースは除く）すべてにパケットを中継します。
2. グループが存在しないインタフェースを刈り込みます。
   グループが存在しない場合は，DVMRP-Prune を送信します。
3. 刈り込み動作終了後に，グループ 1 宛てのマルチキャストパケットを送信します。

この動作の流れを次の図に示します。

図 15-28　DVMRP によるマルチキャストパケット中継処理

(3)　近隣検出

DVMRP ルータはマルチキャストができるすべてのインタフェースとトンネルインタフェースに定期的に DVMRP-Probe メッセージを送信します。DVMRP-Probe メッセージは All-DVMRP-RoutersIP マルチキャストグループアドレス宛て (224.0.0.4) に送信します。このメッセージを受信することによって近隣の DVMRP ルータを動的に検出します。

(4) 経路情報の通知

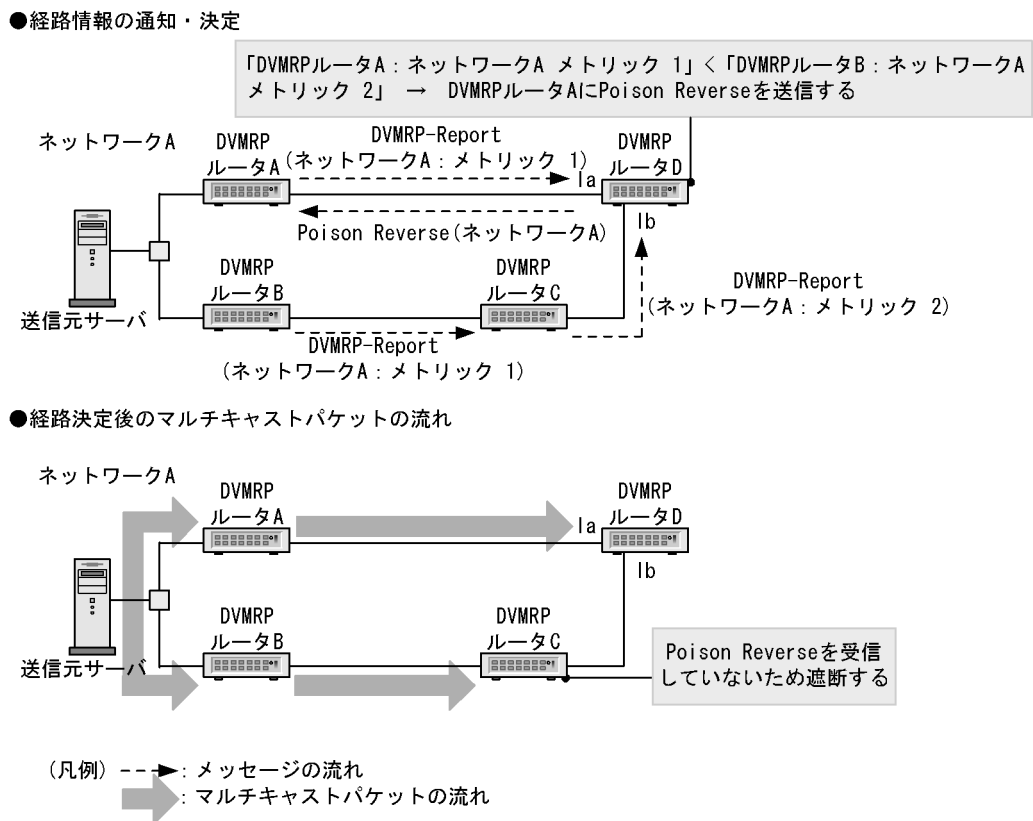
DVMRP ルータはすべての隣接 DVMRP ルータと経路情報通知 (DVMRP-Report) を行います。このメッセージ交換によってユニキャストルーティング情報を得て，マルチキャスト通信の送信元からの最短パスを決定し，各送信者 (送信元ネットワーク) からのマルチキャストパケットの受信インタフェースを決定します。経路情報通知・決定およびマルチキャストパケットの流れを次に示します。

1. 経路情報の通知・決定
   ネットワークに対するルータからの広告で，メトリックがより小さいネットワークに対する受信インタフェースを Ia に決定します。
2. 決定した経路のルータには経路情報を有効にしたことを通知する Poison Reverse を送信します。経路に決定されなかったルータには該当するネットワークに対する Poison Reverse を受信しないため，該当するネットワークを送信元アドレスとするマルチキャストパケットを送信しません。

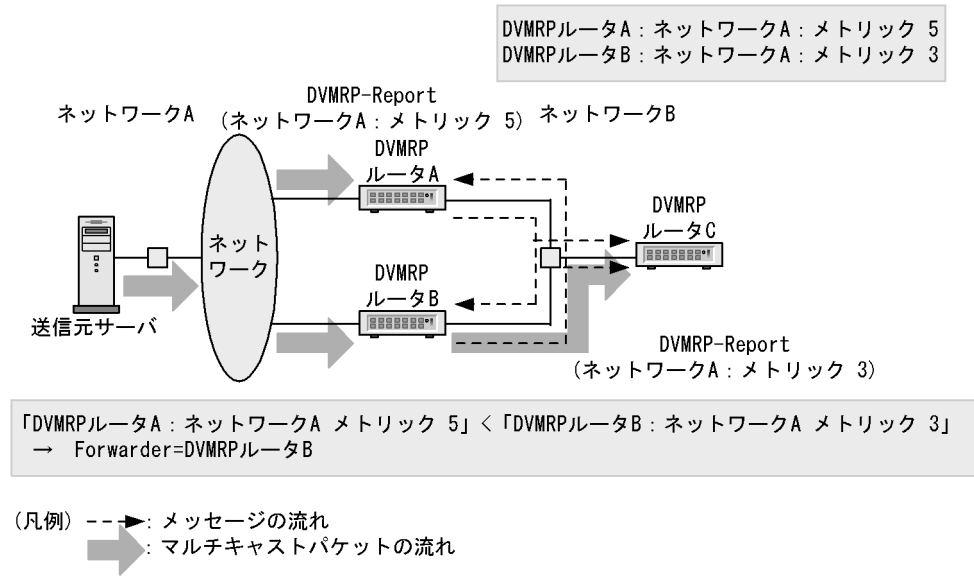
経路情報通知・決定の流れを次の図に示します。

図 15-29　経路情報通知・決定

●経路情報の通知・決定

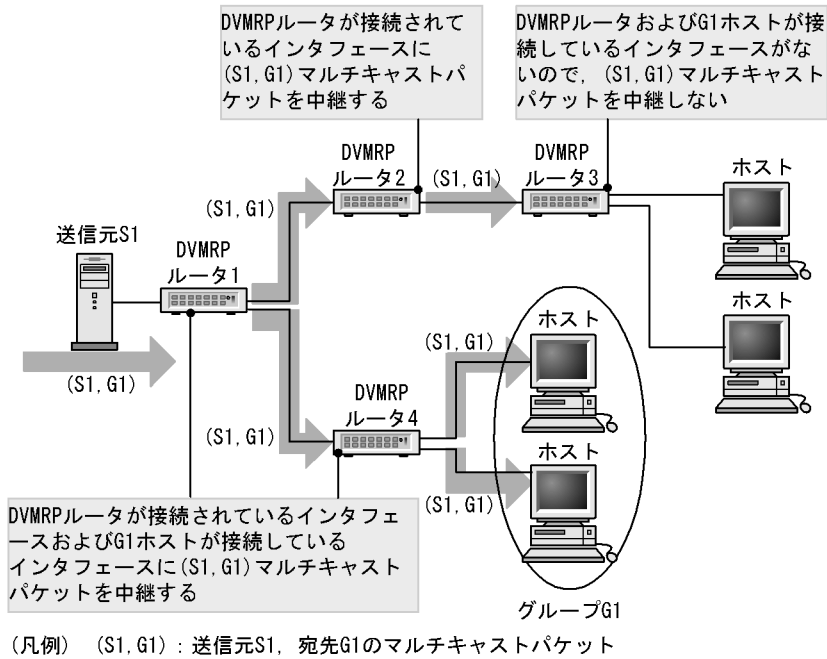
●経路決定後のマルチキャストパケットの流れ

(5) Designated Forwarder の決定

同一 LAN 上に複数の DVMRP ルータが接続している場合，そのネットワークに重複パケットがフォワードされる可能性があります。DVMRP ルータは同一 LAN 上に複数の DVMRP ルータが存在した場合，経路情報 (DVMRP-Report) に含まれるメトリックを参照し，送信元ネットワークに対して最も小さいメトリックを持ったルータが同一 LAN 上にパケットをフォワードする権利を持ちます。もしメトリックが等しい場合，より小さい IP アドレスを持ったルータがフォワードする権利を持ちます。ただし，実際に中継するためには下流ルータから Poison Reverse を受信する必要があります。Designated Forwarder の決定を次の図に示します。

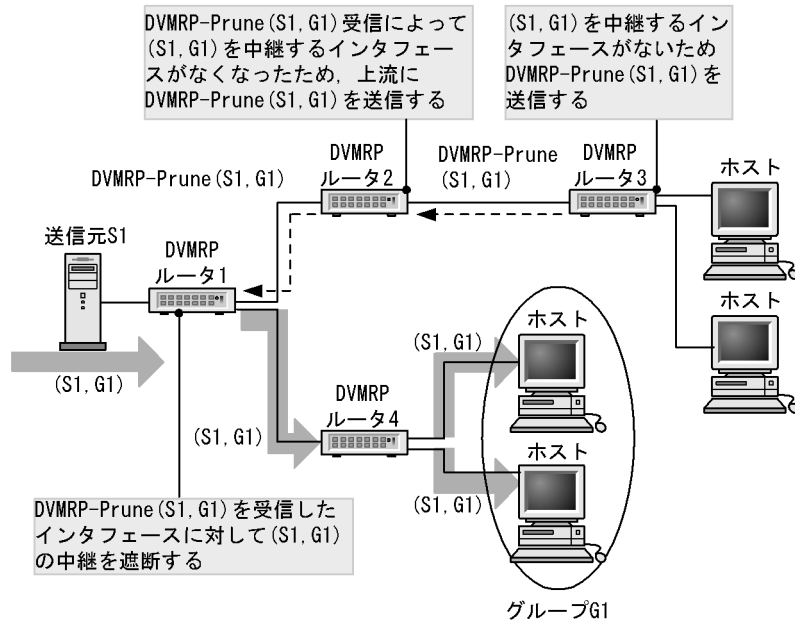
図 15-30　Designated Forwarder の決定

(6) マルチキャスト配送ツリーの刈り込み

(a) 刈り込み前の動作

DVMRP ルータは最初にマルチキャストパケットを受信したとき，中継できるインタフェース (Poison Reverse を送信してきた DVMRP 近隣ルータが存在する，または IGMP メンバーシップ情報があるインタフェース) のすべてを配送ツリーに登録します。中継できるインタフェースがない場合，送信元に対する次ホップルータ (Forwarder) に対して，中継する必要がないことを DVMRP-Prune(刈り込み) メッセージで通知します。DVMRP-Prune メッセージを受信した DVMRP ルータは，あらかじめ登録してあった配送ツリーから DVMRP-Prune メッセージを受信したインタフェースを刈り込みます。マルチキャスト配送ツリーの刈り込み前の動作を次の図に示します。

図 15-31 マルチキャスト配送ツリーの刈り込み前の動作

(b) 刈り込み動作

DVMRP ルータ 3 では，(S1，G1) マルチキャストパケットを中継するインタフェースがないため (S1，G1) マルチキャストパケットを受信したインタフェースに対して DVMRP-Prune(S1，G1) を送信し，自ルータが該当するインタフェースから (S1，G1) マルチキャストパケットを受信する必要がないことを通知します。また，DVMRP ルータ 2 では，DVMRP-Prune(S1,G1) を受信したことによって (S1,G1) マルチキャストパケットを中継するインタフェースがなくなったため (S1,G1) マルチキャストパケットを受信したインタフェースに対して DVMRP-Prune(S1,G1) を送信します。マルチキャスト配送ツリーの刈り込み動作を次の図に示します。

図 15-32　マルチキャスト配送ツリーの刈り込み動作

（凡例）　DVMRP-Prune(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の刈り込み

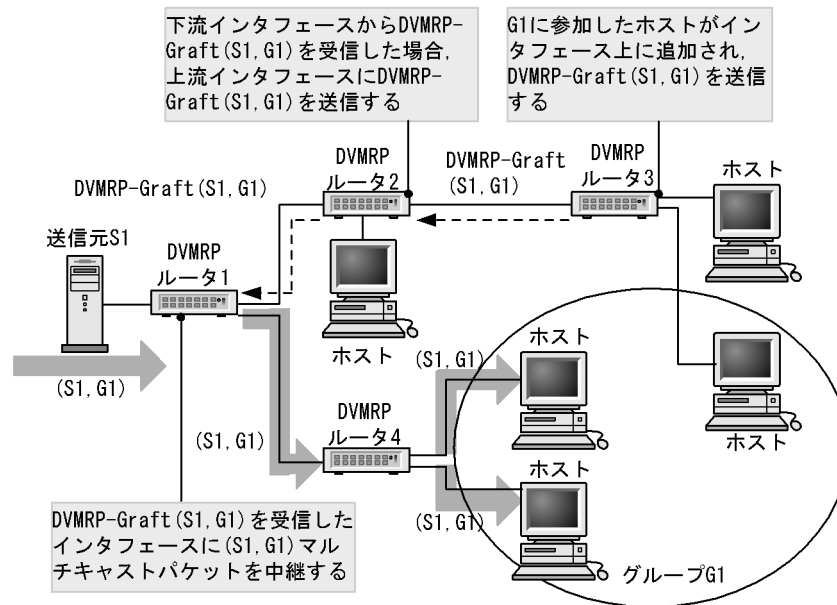
(7) マルチキャスト配送ツリーの再接続

マルチキャスト配送ツリーから刈り込んだツリーには該当する送信元から該当するグループへのパケットは中継しません。しかし刈り込んだツリーに新しくそのマルチキャストグループへの参加があった場合，刈り込んだツリーに再接続 (DVMRP-Graft) メッセージを送信します。DVMRP ルータは DVMRP-Graft メッセージを受信したら配送ツリーにそのインタフェースを追加し，DVMRP-Graft-Ack メッセージを返信します。

(a) 再接続動作

新しくグループに参加したホストがインタフェース上に追加された場合，G1 に対して prune を送信したインタフェースに graft(S1,G1)(この prune(S1，G1) を送信しているため) を送信し，再接続要求をします。DVMRP-Prune(S1,G1) を受信したインタフェースから DVMRP-Graft(S1,G1) を受信した場合，DVMRP-Prune(S1,G1) を送信したインタフェースに DVMRP-Graft(S1,G1) を送信します。

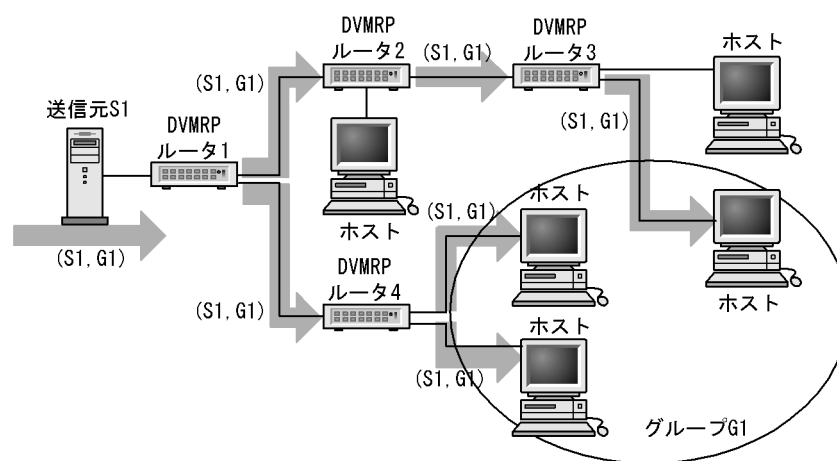
「図 15-32　マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から新しくそのマルチキャストグループに参加があった場合のマルチキャスト配送ツリーの再接続動作を次の図に示します。

図 15-33　マルチキャスト配送ツリーの再接続動作

（凡例）　(S1,G1)：送信元S1，宛先G1のマルチキャストパケット
　　　　DVMRP-Graft(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の再接続

(b) 再接続後のマルチキャストパケットの流れ

DVMRP ルータ 1 には (S1.G1) マルチキャストパケットが中継されているため，DVMRP-Graft(S1,G1) を受信したインタフェースに (S1,G1) マルチキャストパケットを中継します。

「図 15-32　マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から新しくそのマルチキャストグループに参加があった場合の，マルチキャスト配送ツリーの再接続後の動作を次の図に示します。

図 15-34　マルチキャスト配送ツリーの再接続後の動作

（凡例）　(S1,G1)：送信元S1，宛先G1のマルチキャストパケット

(8) DVMRP タイマ仕様

DVMRP が使用するタイマ値を次の表に示します。

表 15-17　DVMRP タイマ

タイマ	値 (秒)
DVMRP-Probe 周期	10
近隣タイムアウト	35
DVMRP-Report 周期	60
Hold Down	120 2 × DVMRP-Report 周期
Prune Life Time	180 DVMRP-Prune を受信している場合は，受信している DVMRP-Prune の Life time の最小値

注　DVMRP タイマの値は変更できない。

15.5 IPv4 マルチキャストソフト処理パケット制御機能

IPv4 マルチキャストソフト処理パケット制御機能とは，本装置が受信するマルチキャストデータパケットを，コンフィグレーションで設定した受信要因と受信パケット数に従って，制御することで，マルチキャストパケット受信による本装置の輻輳を抑止する機能です。なお，当機能は中継パケットには影響ありません。

15.5.1 パケット制御対象受信要因

パケット制御の対象受信要因とその内容を次の表に示します。

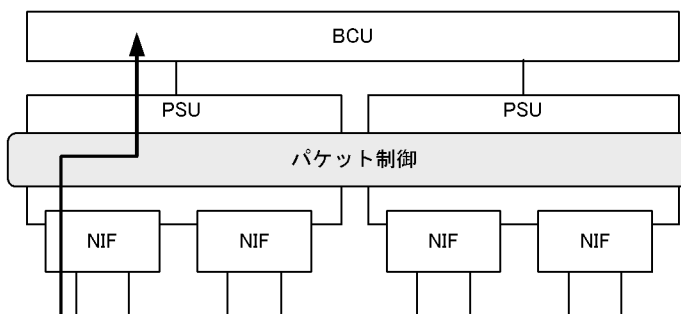
表 15-18 パケット制御対象受信要因

パケット受信要因	内容
wrong-incoming-interface	ハードウェアの IP マルチキャスト中継エントリに登録済みのエントリと一致したマルチキャストデータパケットを別のインタフェースから受信した場合に発生する要因
cache-misshit	ハードウェアの IP マルチキャスト中継エントリに存在しないマルチキャストデータパケットを受信した場合に発生する要因
register-request	first-hop-router において，受信したマルチキャストパケットを Register パケットとしてランデブーポイントに送信する場合に発生する要因
register-receive	ランデブーポイントにおいて，Register パケット受信した場合に発生する要因

15.5.2 パケット制御【SB-7800S】

(1) パケット制御概略

パケット制御の概略を次の図に示します。

図 15-35 パケット制御概略図

ネットワークインタフェースモジュール（NIF）から受信したソフト処理用データパケットを基本制御モジュール（BCU）に転送する際に，コンフィグレーションによって設定した受信要因と比較し，一致した場合，定義した受信パケット数に従って転送数を制御します。

(2) パケット制御実行単位

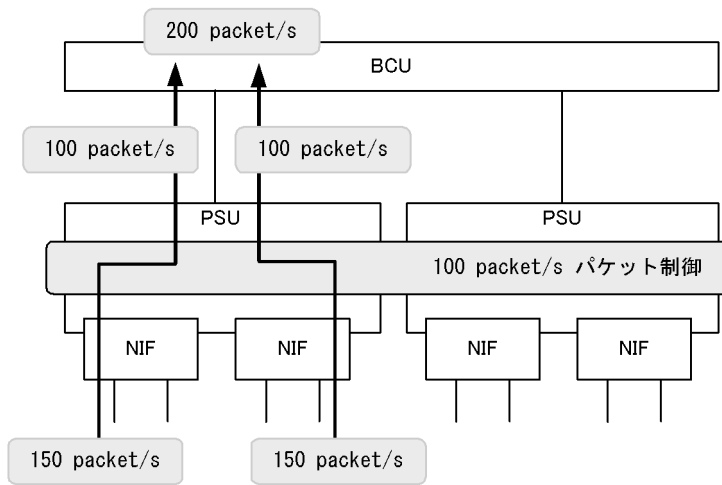
パケット制御を実行する単位は PSU 内蔵型高密度ポート NIF を除き，NIF 単位です。PSU 内蔵型高密度ポート NIF はポート単位にパケット制御を実行します。次に詳細内容を示します。

表 15-19　PSU 内蔵型高密度ポート NIF パケット制御実行単位

<table>
<tr><th>NIF</th><th colspan="5">パケット制御実行単位</th></tr>
<tr><td>S12-1G48S</td><td rowspan="4">右記ポート No.
単位</td><td rowspan="2">0 ～ 11</td><td rowspan="2">12 ～ 23</td><td rowspan="2">24 ～ 35</td><td rowspan="2">36 ～ 47</td></tr>
<tr><td>S12-1G48T</td></tr>
<tr><td>S22-10G4RX</td><td rowspan="2">0</td><td rowspan="2">1</td><td rowspan="2">2</td><td rowspan="2">3</td></tr>
<tr><td>S33-10G4RX</td></tr>
</table>

(3) パケット制御例

パケット制御例を次の図に示します。

図 15-36　パケット制御例

- コンフィグレーションによって,「100 packet/s」でパケット制御実行を指示
- 異なる NIF の 2 インタフェースから 150 packet/s でソフト処理用パケットを受信する
- NIF 単位にパケット制御が実行され，BCU には 200 packet/s でパケットが転送される

(4) ソフト処理パケット制御機能使用時の注意事項

搭載する PSU が PSU-1 または PSU-2 の場合,「表 15-18　パケット制御対象受信要因」の「register-receive」はパケット制御の対象外となり，コンフィグレーションで設定しても受信パケットの転送数は制御されません。

15.5.3　パケット制御【SB-5400S】

(1) パケット制御概略

パケット制御の概略を次の図に示します。

図 15-37　パケット制御概略図

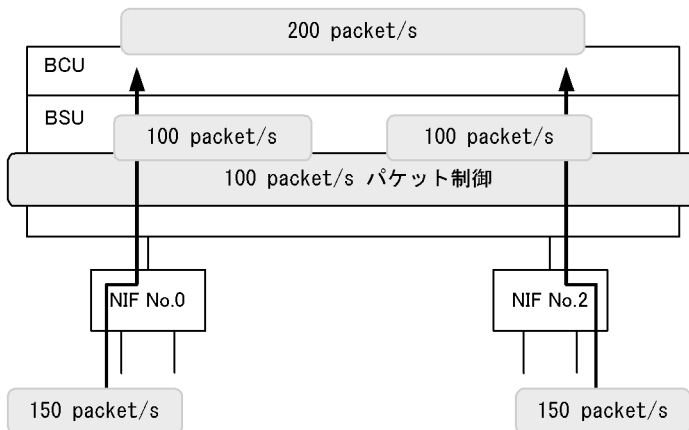
ネットワークインタフェースモジュール（NIF）から受信したソフト処理用データパケットを基本制御モジュール（BCU）に転送する際に，コンフィグレーションによって設定した受信要因と比較し，一致した場合，定義した受信パケット数に従って転送数を制御します。

(2) パケット制御実行単位

パケット制御を実行する単位は NIF を搭載するスロット位置によって異なります。パケット制御はスロット位置 0 と 1，2 と 3 を制御単位として実行します。

(3) パケット制御例

パケット制御例を次の図に示します。

図 15-38　パケット制御例

- コンフィグレーションによって，「100 packet/s」でパケット制御実行を指示
- 異なる NIF（搭載スロット NO.0 と 2）の 2 インタフェースから 150 packet/s でソフト処理用パケットを受信する
- NIF を搭載するスロット位置が 0 と 2 のため各 NIF 単位にパケット制御が実行され，BCU には 200 packet/s でパケットが転送される

(4) ソフト処理パケット制御機能使用時の注意事項

搭載する BSU が BSU-C1 の場合，「表 15-18　パケット制御対象受信要因」の「register-receive」はパケット制御の対象外となり，コンフィグレーションで設定しても受信パケットの転送数は制御されません。

15.6 ネットワーク設計の考え方

15.6.1 IPv4 マルチキャスト中継

本装置でマルチキャストパケットを中継する場合には次の点に注意してください。

(1) プロトコル共通

(a) ソフトウェア中継処理時のパケットロス

本装置は，最初のマルチキャストパケット受信でマルチキャスト通信を行うためのマルチキャスト中継エントリをハードウェアに設定します。マルチキャスト中継エントリを作成するまでの間ソフトウェアでマルチキャストパケットを中継するため，マルチキャスト通信のトラフィック量によっては一時的にパケットをロスする場合があります (PIM-SSM を除く)。

(b) プロトコルの混在

本装置は，PIM-DM，PIM-SM，DVMRP の混在システムをサポートしていません。したがって，全装置のマルチキャストプロトコル (PIM-DM，PIM-SM，DVMRP) を統一して使用してください。PIM-SSM は PIM-SM の拡張機能なので，PIM-SM と PIM-SSM は混在できます。

(c) 二重化装置での系切替に伴う中継断

本装置は，二重化装置による運用で現用系から待機系に切り替わる場合は，マルチキャスト経路情報を再学習するまでマルチキャスト通信が停止するので注意してください。

ただし，IPv4 PIM-SM の場合，コンフィグレーションによってマルチキャスト通信を停止することなく系切替ができます。

(d) ルーティングプログラムの再起動に伴う中継断

restart ipv4-multicast コマンド実行による IP マルチキャストルーティングプログラムの再起動を行う場合は，マルチキャスト経路情報を再学習するまでマルチキャスト通信が停止するので注意してください。

(e) ハードウェア中継切り替え時のパケット追い越し

本装置ではハードウェアへのマルチキャスト中継エントリの設定が完了すると，それまでのソフトウェアによるマルチキャストパケットの中継処理がハードウェア中継へと切り替わります。このときに一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります (PIM-SSM を除く)。

(2) PIM-SM および PIM-SSM の使用

(a) 動作インタフェース

IP アドレスのマスク長が 8 ビットから 30 ビットのインタフェース上で動作します。ポイント - ポイント型の回線上で動作させる場合，自インタフェースと相手インタフェースの IP アドレスのサブネットを同じにしてください。

(b) タイミングによるパケット追い越し

本装置で送信者からのマルチキャストデータと受信者側からの PIM-Join メッセージを同時に受信した場合，タイミングによっては一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります。

（3） PIM-SM の使用

PIM-SM を使用する場合は次の点に注意してください。

（a） パス切り替え時の二重中継またはパケットロス

本装置は，ランデブーポイント経由でのマルチキャストパケット中継時およびランデブーポイント経由から最短パス経由への切り替え時，一時的に二重中継またはパケットロスが発生する場合があります。

ランデブーポイント経由のマルチキャストパケットの中継動作およびランデブーポイント経由から最短パス経由切り替え動作は「15.4.2　IPv4 PIM-SM」を参照してください。

（b） 装置アドレス到達可能性

本装置をランデブーポイントおよびブートストラップルータとして使用する場合，装置管理情報のローカルアドレスで定義された IPv4 アドレスがランデブーポイントとブートストラップルータのアドレスになります。この装置管理情報のローカルアドレスはマルチキャスト通信する全装置でユニキャストでのルート認識および通信ができる必要があります。

（c） PIM-Register メッセージのチェックサム

本装置以外の装置と混在するシステム構成では，PIM-Register メッセージ (カプセル化パケット) のチェックサムの計算範囲の相違によってマルチキャスト通信ができない場合があります。ランデブーポイントで Register メッセージがチェックサムエラーによってマルチキャスト中継しない場合は，本装置のコンフィグレーションで PIM チェックサムを計算する範囲を変更してください。詳細は，マニュアル「コンフィグレーションコマンドレファレンス Vol.1」の pim コマンドを参照してください。

（d） 静的ランデブーポイント

静的ランデブーポイントは，BSR を使用しないでランデブーポイントを指定する機能です。静的ランデブーポイントはコンフィグレーションによって定義します。

静的ランデブーポイントは BSR から Bootstrap メッセージによって広告されたランデブーポイント候補との共存もできます。共存時，静的ランデブーポイントは BSR から Bootstrap メッセージによって広告されたランデブーポイント候補よりも優先されます。

なお，ランデブーポイント候補のルータは，ランデブーポイントルータアドレスが自アドレスであることを認識することでランデブーポイントとして動作します。したがって，BSR を使用しないで静的ランデブーポイントを使ってネットワークを設計する場合は，ランデブーポイント候補のルータでも静的ランデブーポイントの定義が必要です。

また，静的ランデブーポイントを使用する場合，同一ネットワーク上の全ルータに対して同じ定義をする必要があります。

（e） 系切替時の nonstop forwarding【SB-7800S】

PIM-SM に系切替時に通信を継続することが可能な nonstop forwarding 機能をサポートしています。

本機能は，コンフィグレーションで nonstop-forwarding を設定した場合だけ有効になります。

nonstop forwarding 機能使用時の注意事項を次に示します。

1. 系切替後のマルチキャスト中継エントリの再学習完了時間は約 450 秒です。再学習の開始と終了は運用ログとして出力します。運用ログの詳細については，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. 系切替後のマルチキャスト中継エントリの再学習状況は，次に示す運用コマンドで確認できます。各コマンドの詳細については，マニュアル「運用コマンドレファレンス Vol.2」を参照してください。

- show ip mroute
- show ip mcache
- show ip pim mcache

3. 系切替後のマルチキャスト中継エントリの再学習中に，次に示す運用コマンドのどちらかを実行すると，nonstop forwarding が無効になり，該当するマルチキャスト中継エントリを再学習するまでの間マルチキャスト中継が一時的に停止します。
   - restart ipv4-multicast
   - clear ip mroute *
4. 系切替を行うルータおよびその近隣のルータは，ユニキャスト経路制御プロトコルのグレースフルリスタート機能を有効にしてください。グレースフルリスタートが無効な場合は，系切替直後 PIM メッセージの送受信が正しく行われないため，マルチキャスト中継が一時的に中断することがあります。
5. 系切替を行うルータの近隣ルータは，Generation ID オプションをサポート（RFC4601 および draft-ietf-pim-sm-bsr-07.txt に準拠）している装置を設置してください。近隣ルータが Generation ID オプションをサポートしていない場合は，系切替直後 PIM メッセージの送受信が正しく行われないため，マルチキャスト中継が一時的に中断することがあります。Generation ID オプションの詳細は，「15.4.2　IPv4 PIM-SM （3）近隣検出」を参照してください。
6. nonstop forwarding が有効な状態で系切替したあと，マルチキャスト中継エントリを再学習している間，次の場合にパケットロスが発生することがあります。ただし，マルチキャスト中継エントリの再学習が終了したあとは次に示すパケットロスは発生しません。
   - 中継対象のマルチキャスト中継エントリの下流インタフェースに，カプセル化インタフェースが含まれている場合（ランデブーポイント情報を学習するまでカプセル化インタフェースへの中継が止まります）。
   - ランデブーポイント経由の中継が最短パス経由の中継に遷移している途中で，系切替を行った場合（最短パス経由の中継への遷移完了後，パケットロスしなくなります）。
   - ランデブーポイントルータを系切替したときに，新たなグループ参加要求を受信した場合（最短パス経由の中継への遷移完了後，パケットロスしなくなります）。
   - 中継対象のマルチキャスト中継エントリの上流インタフェースが変更された場合（新しい最短パス経由の中継への遷移完了後，パケットロスしなくなります）。
   - 再学習中に閉塞状態の PSU/NIF を運用状態にした場合，該当する PSU/NIF で下流インタフェースが VLAN またはリンクアグリゲーションとなる場合で，次に示す条件をすべて満たしているとき（マルチキャスト中継エントリの再学習終了後，パケットロスしなくなります）。
     ・該当する VLAN またはリンクアグリゲーションが複数 PSU にわたっている場合
     ・該当する VLAN またはリンクアグリゲーションの閉塞状態である PSU/NIF を運用状態にした場合
   - nonstop forwarding が有効な状態で上流方向へ PIM Join/Prune メッセージを送信する装置を系切替した場合，グレースフルリスタート開始後にすべてのユニキャスト経路を BCU のユニキャストルーティングテーブルに設定するまでの時間が，PIM Join/Prune メッセージ送信間隔の 1.5 倍以上になるとき（全ユニキャスト経路を BCU のユニキャストルーティングテーブルへ設定終了し，該当する装置が上流方向へ PIM Join/Prune メッセージを送付したあと，パケットロスしなくなります）。系切替装置で PIM Join/Prune メッセージ送信間隔を 130 秒以上に設定することで，このパケットロスを防ぐことができます。ただし，この設定をしても，BGP により多数の近隣装置と大量の経路情報を交換する場合やグレースフルリスタートの設定によっては，パケットロスするおそれがあります。この場合は，系切替対象装置に送信元アドレスおよびランデブーポイント装置アドレスへのスタティック経路を最低の優先度で設定してから系切替してください。
7. nonstop forwarding が有効な状態で系切替したあと，マルチキャスト中継エントリを再学習している間，次に示す意図しない中継が発生することがあります。ただし，マルチキャスト中継エントリの再学習が終了したあとは，意図しない中継は発生しません。

- マルチキャストデータの二重中継が発生した場合，その解消に時間がかかることがあります（BCU がマルチキャスト経路情報を再学習すると，PIM Assert により二重中継が抑制されます）。
- 中継対象のマルチキャスト中継エントリのインタフェースに障害が発生し，その後回復した場合，再学習に関係なく中継を再開することがあります。
- 中継対象のマルチキャスト中継エントリのインタフェースをコンフィグレーションまたはプロトコル処理によって削除した場合，中継が停止しないことがあります。
- ランデブーポイント経由の中継が最短パス経由の中継に遷移している途中，両方から二重にパケット中継が行われることがあります（最短パスの配送木への遷移完了後，二重パケット中継はなくなります）。

8. nonstop forwarding が有効な状態でランデブーポイントルータを系切替した場合，マルチキャスト中継エントリを再学習している間でも，PIM Register パケット受信によってソフトウェア中継処理が呼び出される場合は，ipMRoutePkts カウンタが加算されます。
9. nonstop forwarding が有効な状態で系切替したあと，マルチキャスト中継エントリを再学習している間は，マルチキャスト中継エントリの無通信監視を行わず，再学習終了時に未学習のマルチキャスト中継エントリを削除します。そのため無通信エントリ保持時間を再学習期間よりも長く設定していても，系切替後の再学習終了後にマルチキャスト中継エントリが保持されません。
10. nonstop forwarding が有効な状態で BSR を系切替した場合，マルチキャスト中継エントリ再学習期間中は PIM Candidate-RP-Advertisement メッセージの受信と同時に PIM Bootstrap メッセージを広告します。そのため同期間中は，通常の 60 秒間隔よりも短い間隔で PIM Bootstrap メッセージを広告します。
11. nonstop forwarding が有効な状態でランデブーポイントを系切替した場合，マルチキャスト中継エントリ再学習期間中は PIM Candidate-RP-Advertisement メッセージのランデブーポイント保持期間を 210 秒（通常は 150 秒）に設定して広告します。
12. nonstop forwarding が有効な状態で系切替したあと，PIM-SM がマルチキャストインタフェースを認識するのに時間が掛かる場合があります。マルチキャストパケット中継には影響ありませんが，運用コマンド show ip pim interface などの表示が正しくなるまで，時間が掛かることがあります。
13. nonstop forwarding が有効な状態で系切替したあと，マルチキャスト中継エントリを再学習している間，PIM-SSM の動作範囲をコンフィグレーションで変更しないでください。マルチキャスト中継エントリ再学習期間中に PIM-SSM 動作範囲をコンフィグレーションで変更し，マルチキャスト中継エントリが PIM-SM から PIM-SSM 経路，または PIM-SSM から PIM-SM 経路となった場合，マルチキャスト中継の動作は保証できません。

（4） PIM-DM の使用

IP アドレスのマスク長が 8 ビットから 30 ビットのインタフェース上で動作します。ポイント - ポイント型の回線上で動作させる場合，自インタフェースと相手インタフェースの IP アドレスのサブネットを同じにしてください。

（5） DVMRP の使用

IP アドレスのマスク長が 8 ビットから 30 ビットおよび 32 ビットのインタフェース上で動作します。DVMRP はデフォルトルート "0.0.0.0" をサポートしていません。したがってデフォルトルートによるマルチキャストパケットの中継は動作しません。

15.6.2 冗長経路 (回線障害などによる経路切り替え)

本装置でマルチキャスト経路が冗長経路になっている場合の注意点について説明します。

（1） PIM-SM の使用

PIM-SM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

● 優先経路が切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

```
U＋20秒
```

● 回線障害によって優先経路から冗長経路が切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

```
U＜5の時:5～10秒
U≧5の時:U＋0～50秒
```

● 回線復旧によって冗長経路から優先経路に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

```
0～（送信者方向のHello送信周期＋20）秒　（デフォルトでは30＋20＝50秒）
```

● ランデブーポイントおよび BSR が本装置に切り替わった（障害やコンフィグレーションなどでランデブーポイントおよび BSR を本装置にする）場合，通信再開までには次に示す時間が掛かることがあります。
通信再開までの時間は，ランデブーポイントまたは BSR で異なります。括弧内はデフォルト値を示します。

- ランデブーポイント切り替え時：285 秒＋加入通知時間

```
RP-Holdtime(150秒)＋Query-interval(125秒)＋Query Response Interval(10秒)
＋加入通知時間
```

- BSR 切り替え時：最大で 348 秒＋加入通知時間

```
Bootstrap-Timeout(130秒)＋BS_Rand_Override(5～23秒)＋Bootstrap-Period(60秒)
＋Query-interval(125秒)＋Query Response Interval(10秒)＋加入通知時間
```

● DR が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。

- DR 切り替え時：240 秒＋加入通知時間

```
Hello-Holdtime(105秒)＋Query-interval(125秒)＋Query Response Interval(10秒)
＋加入通知時間
```

障害による冗長経路切り替えだけでなく，構成変更によって意識的に経路切り替えを行った場合も，マルチキャスト通信がこれらの時間停止することがあります。システムの構成変更は計画的に実施してください。

（2） PIM-SSM の使用

PIM-SSM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

● 優先経路が切り替わった場合，通信再開までに次に示す時間が掛かることがあります。

```
U＋20秒
```

● 回線障害により優先経路から冗長経路が切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

```
U＜5の時:5～10秒
U≧5の時:U＋0～135秒
```

● 回線復旧により冗長経路から優先経路に切り戻った場合，通信再開までには次に示す時間が掛かることがあります。

```
0秒
ただし，切り戻りにかかる時間は次に示す時間が掛かります。
U＋0～（送信者方向のHello送信周期＋20）秒 （デフォルトでは30＋20＝50秒）
```

● DR が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。
- DR 切り替え時：240 秒＋加入通知時間

```
Hello-Holdtime(105秒)＋Query-interval(125秒)＋Query Response Interval(10秒)
＋加入通知時間
```

（3） PIM-DM の使用

PIM-DM の場合，冗長経路からのマルチキャストパケット通信切り替え時間は最大 210 秒かかります。

（4） DVMRP の使用

DVMRP の場合，冗長経路からのマルチキャストパケット通信切り替え時間は最大 180 秒かかります。

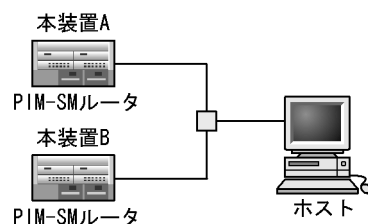
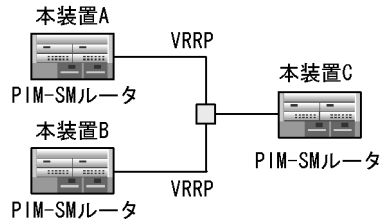
15.6.3 適応ネットワーク構成

マルチキャストはサーバ (送信者) から各グループ (受信者) にデータを配信する 1(送信者) : N(受信者) の片方向通信に適します。IPv4 マルチキャストの適応ネットワーク構成，注意事項を次に示します。

（1） PIM-SM および PIM-SSM 共通

（a） 注意が必要な構成

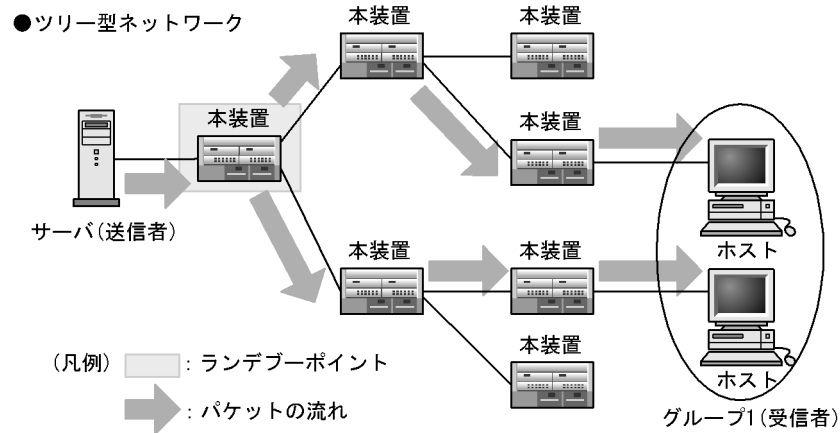
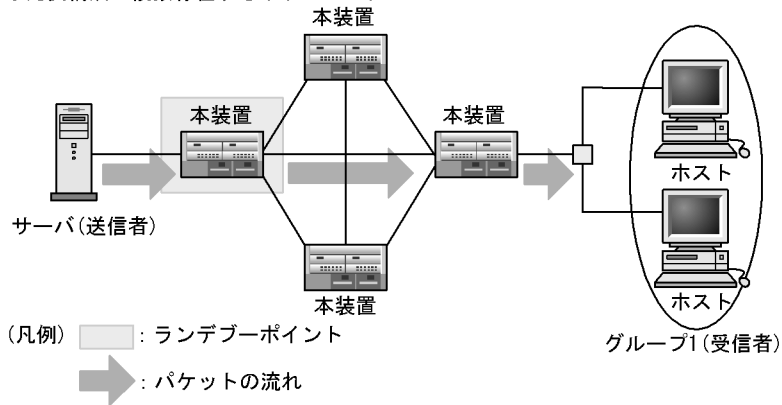
次に示す構成で PIM-SM または PIM-SSM を使用する場合，注意が必要です。

● 次の図に示す構成のようにホストと直接接続するルータが同一ネットワーク上に複数存在するインタフェースには，必ず PIM-SM を動作させてください。
同一ネットワーク上に複数のルータが存在するインタフェースに PIM-SM を動作させずに IGMP だけを動作させた場合は，マルチキャストデータが二重中継される場合があります。

● 次の図に示す構成のように本装置 C が本装置 A と本装置 B に VRRP を設定した仮想インタフェースをゲートウェイとするスタティックルートを設定した環境では，PIM プロトコルが上流ルータを検出できず，マルチキャスト通信ができません。
この構成でマルチキャスト通信する場合は，本装置 C にランデブーポイントアドレスと BSR アドレスとマルチキャストデータ送信元アドレスへのゲートウェイアドレスを本装置 A または本装置 B の実アドレスとするスタティックルートを設定する必要があります。

(2) PIM-SM

(a) 推奨構成

PIM-SM によるネットワークの構成に当たっては，ツリー型ネットワーク構成および冗長経路が存在するネットワーク構成を推奨します。ただし，ランデブーポイントの配置には十分注意してください。ランデブーポイント経由のマルチキャスト通信でのカプセル化処理および最短パス確立後のカプセル化抑止パケットの処理は，各ルータに負荷がかかるため，ランデブーポイントは送信者の直近に置くことをお勧めします。

PIM-SM 推奨ネットワーク構成を次の図に示します。

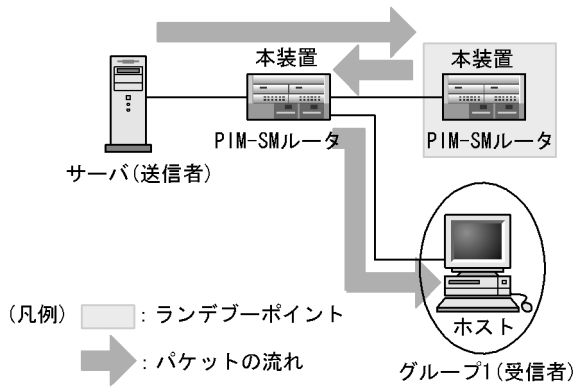
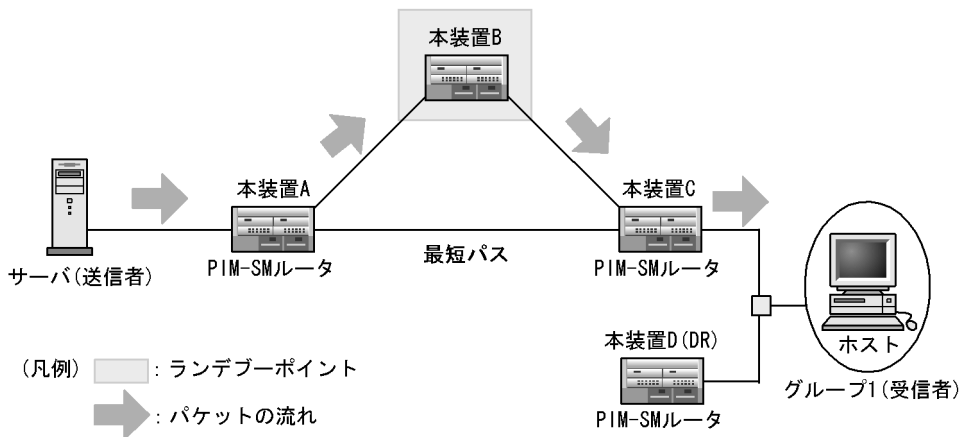
図 15-39　PIM-SM 推奨ネットワーク構成

(b) 注意が必要な構成

次に示す構成は注意が必要です。

● 次の図に示すように送信者と直接接続するルータが同一ネットワーク上に 2 台以上存在する構成で，どれかをランデブーポイントとする場合は，ランデブーポイントが DR になるようにしてください。
ランデブーポイント以外を DR にした場合，DR からランデブーポイントに対し PIM-Register メッセージを送信するため，本装置 A，B に負荷がかかります。また，PIM-Register メッセージ中のマルチキャストパケットを中継するときに，ランデブーポイントでパケットロスが発生するおそれがあります。なお，ランデブーポイントを DR にした場合は，PIM-Register メッセージによるカプセル化は行いません。

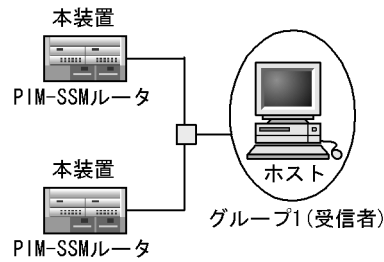
(c) 不適応な構成

次に示す構成で PIM-SM は使用しないでください。

● 送信者とランデブーポイントの間に受信者が存在する構成
次に示す構成でサーバからグループ 1 のマルチキャスト通信を行う場合，ランデブーポイント経由の中継が効率よく行えません。

● DR である PIM-SM ルータがマルチキャストグループ (受信者) の存在する回線に対してだけ接続している構成
次に示す構成でグループ 1 宛てのマルチキャスト通信をした場合，送信者とグループ 1 間で最短パスが確立しないことがあります。このため，ランデブーポイントを経由するマルチキャスト通信が続くことになります。
この場合，DR である本装置 D はグループ 1 が存在する回線とは別の回線でランデブーポイントや送信者に至る経路を確保するようにネットワーク構築してください。

(3) PIM-SSM

(a) 注意が必要な構成

次に示す構成は注意が必要です。

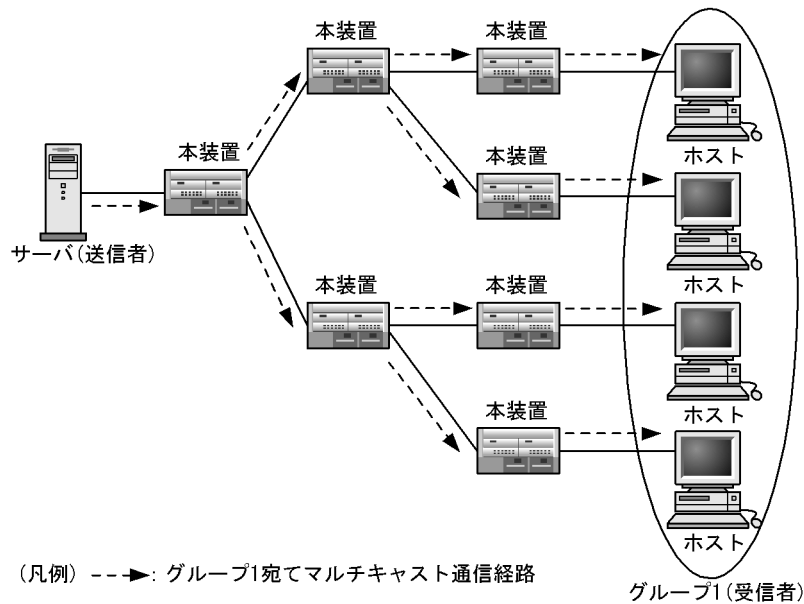
● マルチキャストグループ (受信者) と同一回線上に複数の PIM-SSM ルータが動作する構成
次に示す構成で IGMPv2 の PIM-SSM を動作させる場合は，同一回線上の全ルータのコンフィグレーションコマンド ssm(pim sparse モード) および ssm-join(multicast モード) を設定してください。

(b)　端末側に複数のアドレスを設定したときの注意事項

SSM 通信時，データ送信を行う端末に複数のアドレスを付与して運用する場合，送信されるデータの送信元アドレスが本装置に設定した ssm-join の送信元アドレス情報と一致するようにしてください。特に，DHCP などのアドレス自動設定機能を使用した場合は，端末側が自動設定されたアドレスを使用して通信を行うことがあります。

(4)　PIM-DM

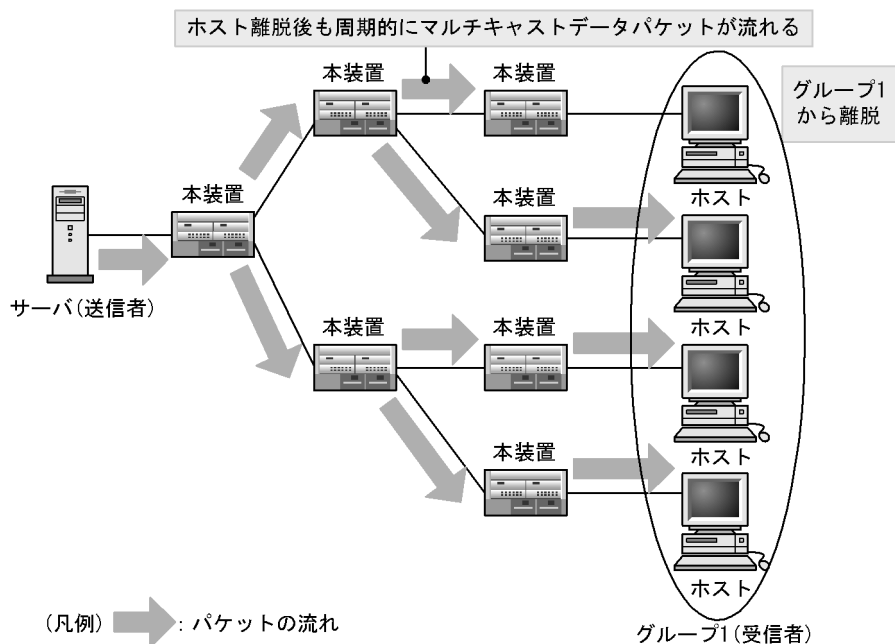
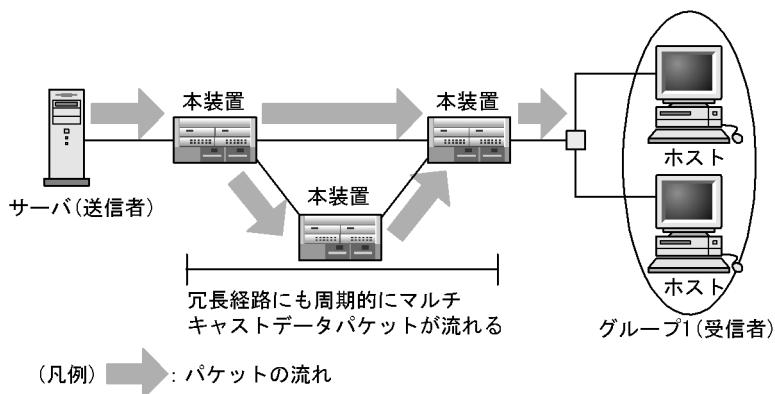
(a)　推奨構成

PIM-DM 推奨ネットワーク構成を次の図に示します。

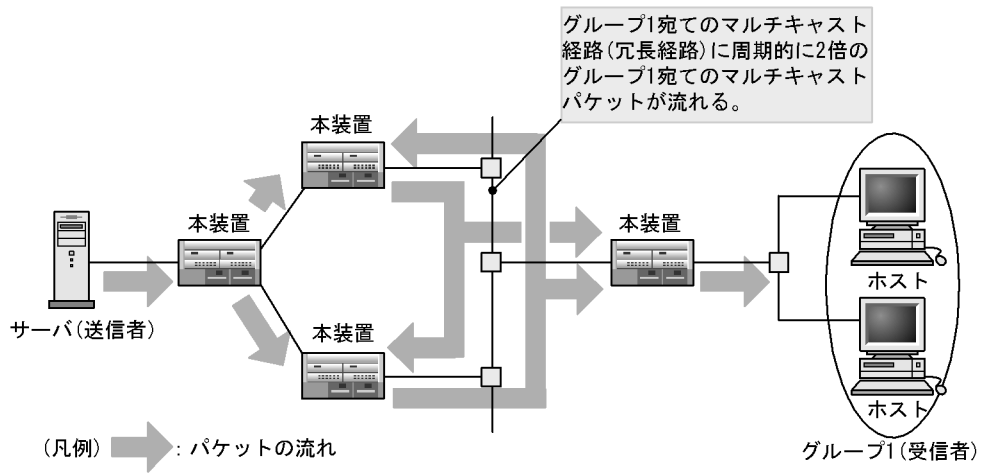
図 15-40　PIM-DM 推奨ネットワーク構成

(b)　注意が必要な構成

次に示す構成は注意が必要です。

● ホストがマルチキャストグループから離脱したあと，マルチキャストグループが存在しないネットワークにも周期的（約 3 分）にマルチキャストデータパケットが送信されます。

ホスト離脱後も周期的にマルチキャストデータパケットが流れる
本装置
グループ1
から離脱
ホスト
サーバ(送信者)
（凡例） : パケットの流れ
グループ1(受信者)

● 冗長構成が存在する場合，冗長経路にマルチキャストデータパケットが周期的（約 3 分）に流れます。

(c) 不適応な構成

次に示す構成で PIM-DM は使用しないでください。

● PIM-DM は複数の冗長経路が存在するネットワーク構成では周期的にすべての経路でマルチキャスト通信を行います。ネットワーク全体に負荷が発生するので，PIM-DM ではなく PIM-SM を使用してください。

(5) DVMRP

PIM-DM 推奨ネットワーク構成と同じです。

16 IPv6 パケット中継

IPv6 ネットワークには通信機能，IP パケット中継，フィルタリング，ロードバランスなどいろいろな機能があります。この章では IPv6 パケット中継について説明します。

16.1 IPv6 概説

本装置がサポートしている IPv6 には次の特長があります。

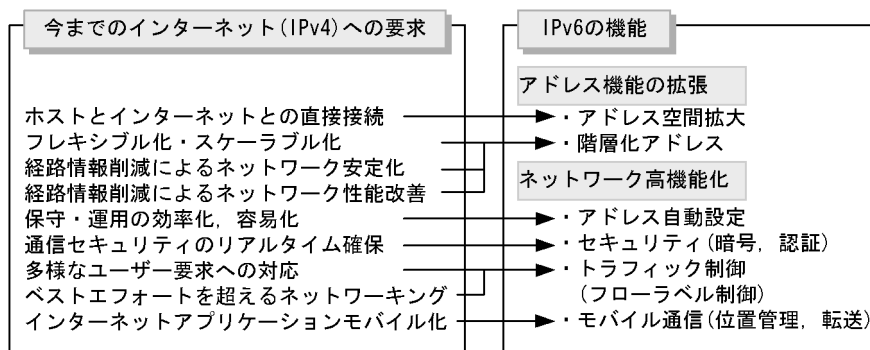
● IP アドレスの枯渇問題を解決できる

IPv4 では IP アドレスが不足するという問題がありました。しかし，IPv6 は 128 ビットの IP アドレスを利用できます。今後予想される携帯電話や情報家電品などへの IP アドレスにも対応できます。

● 基本機能にはセキュリティに対する機能やアドレス自動設定機能が含まれる

IPv6 の基本仕様にはパケットの暗号化やパケットにラベルを付けて通信の優先度を制御する機能や，ネットワークに接続するときにアドレスを自動設定する機能も含まれています。このため，より高品質で高速なネットワーク運用ができます。

IPv6 の必要性を次の図に示します。

図 16-1 IPv6 の必要性

16.2　アドレッシング

IPv6 は IPv4 と比較して次のような特長があります。

- **アドレス構造を拡張している**
  アドレス長が 32 ビットから 128 ビットに拡張されています。このため，ノードへ割り当てができるアドレス数がほぼ無限となり，IPv4 で問題となっていたアドレス枯渇問題が解消されます。また，アドレス構造階層のレベル数が増加したため，新しいアドレスを定義できるようになります。
- **ヘッダ形式を単純化している**
  IPv4 と比較してヘッダフィールドが簡略化され，プロトコル処理のオーバヘッドが減少しています。
- **拡張ヘッダとオプションヘッダを強化している**
  転送効率の向上，オプションの長さ制限の緩和，また，オプション拡張が容易です。
- **フローラベルを設定できる**
  特定のトラフィックフローを識別するためのラベル付けができます。
- **認証と機密保持機能をサポートしている**
  パケット中に認証，データ整合性確認，データ機密保持などの機能がサポートされています。

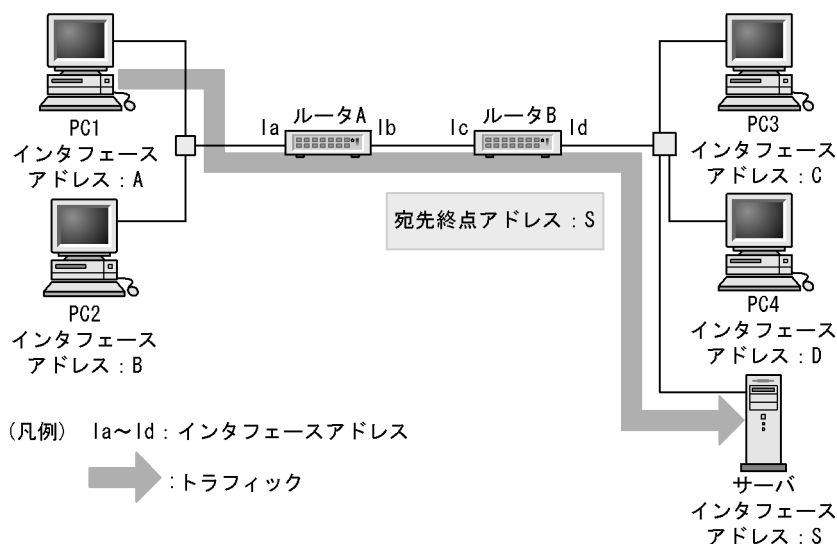
本装置で使用する IPv6 ネットワークのアドレッシングについて概要を示します。

16.2.1　IPv6 アドレス

IPv6 アドレスにはユニキャスト，エニキャスト，マルチキャストの 3 種類のアドレス形式が定義されています。

(1)　ユニキャストアドレス

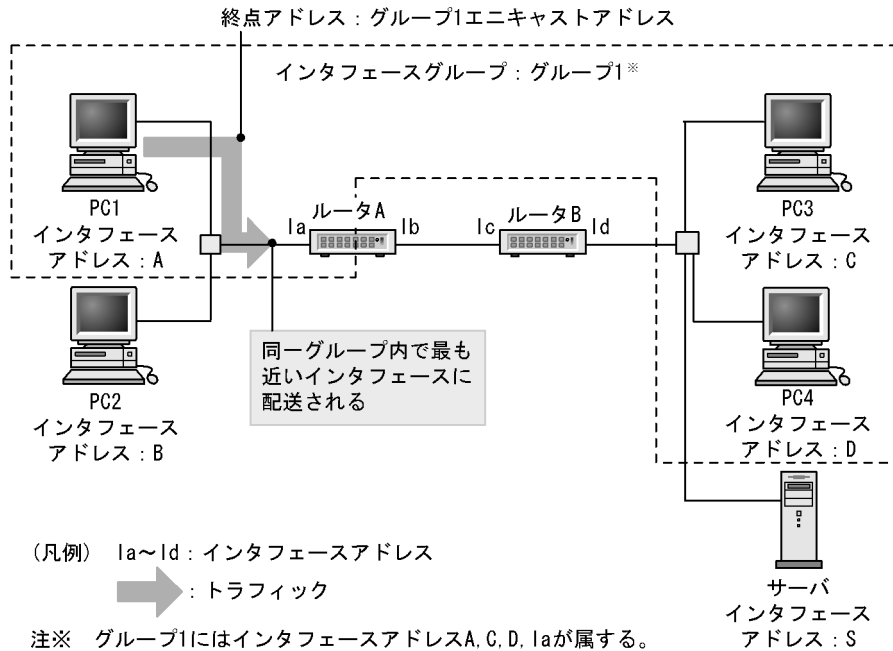
単一のインタフェースを示すアドレスです。終点アドレスがユニキャストアドレスのパケットは，そのアドレスが示すインタフェースに配送されます。ユニキャストアドレス通信を次の図に示します。

図 16-2　ユニキャストアドレス通信

(2)　エニキャストアドレス

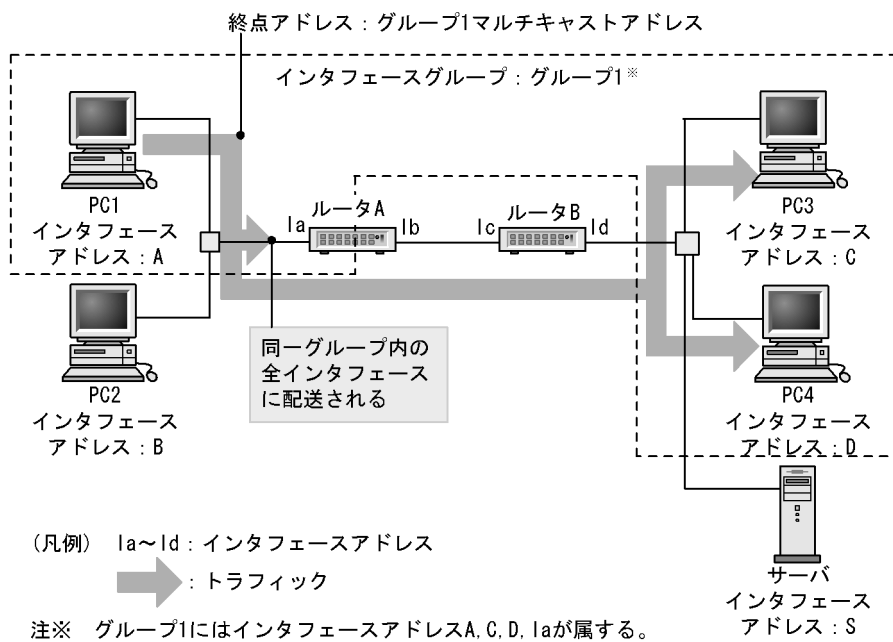
インタフェースの集合を示すアドレスです。終点アドレスがエニキャストアドレスのパケットは，インタフェース集合のうち，経路制御プロトコルによって測定された距離の最も近いインタフェースに配送され

ます。なお，本装置ではエニキャストアドレスは未サポートです。エニキャストアドレス通信を次の図に示します。

図 16-3　エニキャストアドレス通信

終点アドレス：グループ1エニキャストアドレス
インタフェースグループ：グループ1※
PC1
インタフェース
アドレス：A
PC2
インタフェース
アドレス：B
ルータA
Ia
Ib
Ic
ルータB
Id
PC3
インタフェース
アドレス：C
PC4
インタフェース
アドレス：D
同一グループ内で最も
近いインタフェースに
配送される
サーバ
インタフェース
アドレス：S
（凡例） Ia～Id：インタフェースアドレス
：トラフィック
注※　グループ1にはインタフェースアドレスA，C，D，Iaが属する。

（3） マルチキャストアドレス

インタフェースの集合を示すアドレスです。終点アドレスがマルチキャストアドレスのパケットは，そのアドレスが示すインタフェース集合のすべてのインタフェースに配送されます。マルチキャストアドレス通信を次の図に示します。

図 16-4　マルチキャストアドレス通信

16.2.2 アドレス表記方法

IPv6 のアドレスは 128 ビット長です。実際に表記するときの方法を次に示します。

- 16 進数で 16 ビットごとにコロン " : " で区切った形式で表記します。
  （例） 3ffe:0501:0811:ff02:0000:08ff:fe8b:3090
- 16 進数の先頭にくる "0" は省略できます。
  （例） 3ffe:501:811:ff02:0:8ff:fe8b:3090
- 連続する "0" は二つのコロン "::" に置換できます。ただし，"::" に置換できるのは一つのアドレス表記に 1 か所までと定義されています。
  （例） 次に示す IPv6 アドレスのときの置換方法
  fe80:0000:0000:0000:0000:0000:0000:3090 → fe80::3090
  （例） 2 か所以上の "::" は禁止
  fe80:0000:0000:0000:0000:0000:0000:3090 → fe80::0::3090
- 次に示す形式でアドレスとプレフィックス長を指定できます。
  - IPv6 アドレス／プレフィックス長
  - IPv6 アドレス prefixlen プレフィックス長

  プレフィックス長はアドレス左端から何ビットまでがプレフィックスかを 10 進数で指定します。

16.2.3 アドレスフォーマットプレフィックス

128 ビット長の IPv6 アドレスが複数のサブフィールドに分割されています。先頭ビットは IPv6 アドレスのタイプを識別する役割があり，アドレスフォーマットプレフィックスと呼ばれます。アドレスフォーマットプレフィックスを「図 16-5 アドレスフォーマットプレフィックス」に示します。また，アドレスフォーマットプレフィックスの種類を「表 16-1 アドレスフォーマットプレフィックスの種類」に示します。

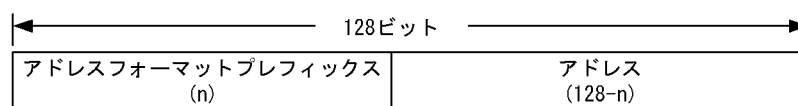
図 16-5 アドレスフォーマットプレフィックス

（ ）内の数字はビット数を示す。

表 16-1 アドレスフォーマットプレフィックスの種類

プレフィックス (2 進数)	割り当て
0000 0000	予備
0000 0001	未割り当て
0000 001	NSAP 割り当て用予約
0000 010	IPX 割り当て用予約
0000 011	未割り当て
0000 1	未割り当て
0001	未割り当て
001	集約可能グローバルユニキャストアドレス
010	未割り当て
011	未割り当て

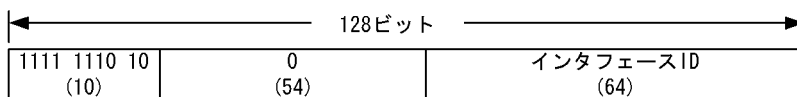
プレフィックス (2 進数)	割り当て
100	未割り当て
101	未割り当て
110	未割り当て
1110	未割り当て
1111 0	未割り当て
1111 10	未割り当て
1111 110	未割り当て
1111 1110 0	未割り当て
1111 1110 10	リンクローカルユニキャストアドレス
1111 1110 11	サイトローカルユニキャストアドレス
1111 1111	マルチキャストアドレス

16.2.4 ユニキャストアドレス

(1) リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80:: で，64 ビットのインタフェース ID 部を含むアドレスを **IPv6 リンクローカルアドレス**と呼びます。IPv6 リンクローカルアドレスは同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータが存在しないときに使用されます。パケットの始点または終点アドレスが IPv6 リンクローカルアドレスの場合，本装置はパケットをほかのリンクに転送することはありません。

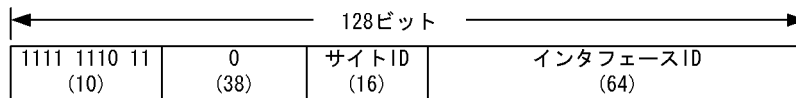
本装置で IPv6 を使用するインタフェースには IPv6 リンクローカルアドレスが必ず一つ設定されます。二つ以上は設定できません。IPv6 リンクローカルアドレスを次の図に示します。

図 16-6 IPv6 リンクローカルアドレス

(2) サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスを **IPv6 サイトローカルアドレス**と呼びます。IPv6 サイトローカルアドレスは，同一組織 (サイト) 内だけで有効なアドレスで，インターネットに接続されていないネットワークで自由に IPv6 アドレスを付ける場合に使用されます。本装置は IPv6 サイトローカルアドレスを「(3) グローバルアドレス」の IPv6 グローバルアドレスとして扱います。そのため，IPv6 サイトローカルアドレスをインタフェースに設定した場合は，IPv6 サイトローカルアドレス情報がサイト外に出ないようにルーティングやフィルタリングを設定してください。IPv6 サイトローカルアドレスを次の図に示します。

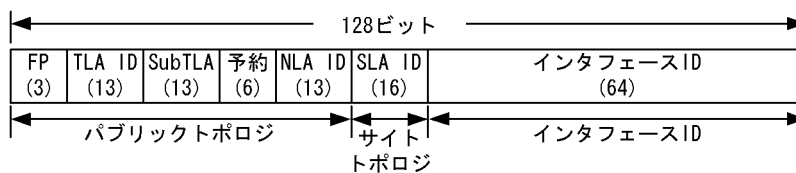
図 16-7　IPv6 サイトローカルアドレス

128ビット

1111 1110 11 (10)	0 (38)	サイトID (16)	インタフェースID (64)

（　）内の数字はビット数を示す。

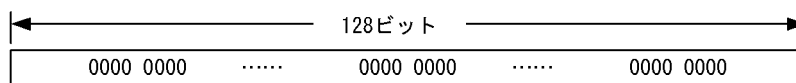
(3)　グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスを **IPv6 グローバルアドレス**と呼びます。IPv6 グローバルアドレスは経路情報の集約を目的とした階層形式で，集約子として TLA ID(Top-Level Aggregation Identifier：最上位階層集約子），Sub-TLA ID(Sub-TLA Identifier：準最上位階層集約子），NLA ID(Next-Level Aggregation Identifier：次階層集約子），SLA ID(Site-Level Aggregation Identifier：組織階層集約子）を持っています。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを介した通信を行う場合に使用されます。パケットの始点アドレスが IPv6 グローバルアドレスの場合，経路情報に従ってパケットが転送されます。IPv6 グローバルアドレスを次の図に示します。

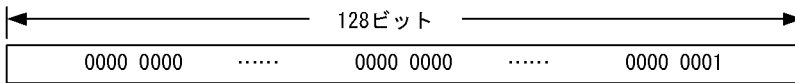
図 16-8　IPv6 グローバルアドレス

（　）内の数字はビット数を示す。

(4)　未指定アドレス

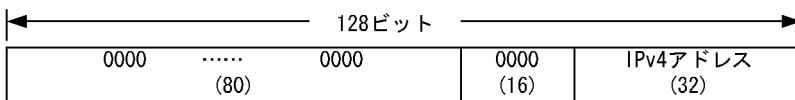
すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または ::) は，**未指定アドレス**と定義されています。未指定アドレスはインタフェースにアドレスが存在しないことを表しています。これは，アドレスの割り当てを受けていないノードの接続開始時などに使用されます。未指定アドレスをノードに対して意図的に割り当てることはできません。未指定アドレスを次の図に示します。

図 16-9　未指定アドレス

(5)　ループバックアドレス

アドレス 0:0:0:0:0:0:0:1(0::1，または ::1) は，**ループバックアドレス**と定義されています。ループバックアドレスは自ノード宛て通信を行うときにパケットの宛先アドレスとして使用されます。ループバックアドレスをインタフェースに対して割り当てることはできません。また，終点アドレスがループバックアドレスの IPv6 パケットは，そのノード外に送信することや，ルータによって転送することは禁止されています。ループバックアドレスを次の図に示します。

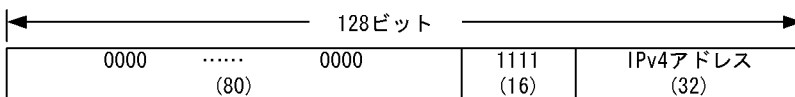
図 16-10　ループバックアドレス

（6） IPv4 互換アドレス

IPv4 互換 IPv6 アドレスは，二つの IPv6 ノードが IPv4 で経路制御されたネットワークで通信するためのアドレスです。下位 32 ビットに IPv4 アドレスを含む特殊なユニキャストアドレスで，IPv4 ネットワークに接続している機器同士が通信を行う場合に使用します。プレフィックスは 96 ビット長ですべて 0 です。IPv4 互換アドレスを次の図に示します。

図 16-11　IPv4 互換アドレス

（　）内の数字はビット数を示す。

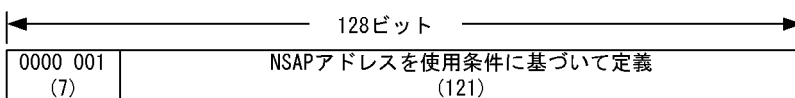
（7） IPv4 射影アドレス

IPv4 射影 IPv6 アドレスは，IPv6 をサポートしていない IPv4 専用ノードで使用されます。IPv4 しかサポートしないホストと IPv6 ホストが通信する場合に IPv6 ホストは IPv4 射影 IPv4 アドレスを使用します。プレフィックスは 96 ビット長で上位 80 ビットの 0 に続き 16 ビットの 1 が設定されます。IPv4 射影アドレスを次の図に示します。

図 16-12　IPv4 射影アドレス

（　）内の数字はビット数を示す。

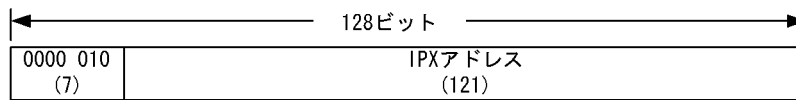
（8） NSAP 互換アドレス

IPv6 で NSAP アドレスを変換して使用するためのアドレス形式です。NSAP をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 001 が定義されています。NSAP 互換アドレスを次の図に示します。

図 16-13　NSAP 互換アドレス

（　）内の数字はビット数を示す。

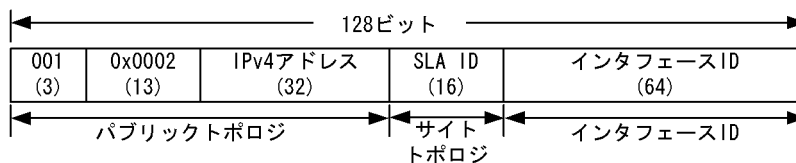
(9) IPX 互換アドレス

IPv6 で IPX アドレスを変換して使用するためのアドレス形式です。IPX をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 010 が定義されています。IPX 互換アドレスを次の図に示します。

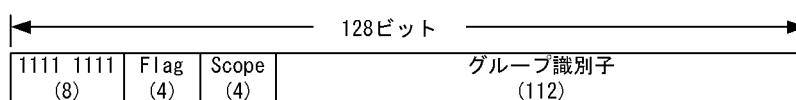
図 16-14　IPX 互換アドレス

(10) 6to4 アドレス

6to4 トンネルで使用するアドレス形式です。6to4 トンネル用として，IANA(Internet Assigned Numbers Authority) から IPv6 グローバルアドレスにおける集約子の一つである TLA ID には 0x0002 が割り当てられています。また，NLA ID には 6to4 トンネルを使用するサイトが持つグローバル・ユニキャスト・IPv4 アドレスが定義されます。

6to4 アドレスを次の図に示します。

図 16-15　6to4 アドレス

16.2.5　マルチキャストアドレス

マルチキャストアドレスは複数のノードの集合体を示すアドレスです。アドレスフォーマットプレフィックスの上位 8 ビットが ff であるアドレスが定義されています。ノードは複数のマルチキャストグループに属することができます。マルチキャストアドレスは，パケットの始点アドレスとして使用することはできません。マルチキャストアドレスには，アドレスフォーマットプレフィックスに続いて，フラグフィールド (4 ビット)，スコープフィールド (4 ビット) およびグループ識別子フィールド (112 ビット) が含まれます。IPv6 マルチキャストアドレスを次の図に示します。

図 16-16　IPv6 マルチキャストアドレス

フラグフィールドの 4 ビットは 1 ビットずつフラグとして定義されています。4 ビット目は T(transient) フラグビットと定義されており，次の値になります。

1. T フラグビットが 0：IANA によって永続的に割り当てられた既知のマルチキャストアドレス

2. T フラグビットが 1：一時的に使用される (非永続的な) マルチキャストアドレス

スコープフィールドは 4 ビットのフラグでマルチキャストグループのスコープを限定するために使用します。マルチキャストアドレスのスコープフィールド値を次の表に示します。

表 16-2 マルチキャストアドレスのスコープフィールド値

値	スコープの範囲
0	予約
1	ノードローカルスコープ
2	リンクローカルスコープ
3	未割り当て
4	未割り当て
5	サイトローカルスコープ
6	未割り当て
7	未割り当て
8	組織ローカルスコープ
9	未割り当て
A	未割り当て
B	未割り当て
C	未割り当て
D	未割り当て
E	グローバルスコープ
F	予約

なお，マルチキャストアドレスには次のようなものがありますが，本装置では 3 〜 5 までのマルチキャストアドレスはサポートしていません。

1. ノードローカルマルチキャストアドレス
2. リンクローカルマルチキャストアドレス
3. サイトローカルマルチキャストアドレス
4. 組織ローカルマルチキャストアドレス
5. グローバルマルチキャストアドレス

(1) 予約マルチキャストアドレス

次に示すマルチキャストアドレスはあらかじめ予約されており，どのマルチキャストグループにも割り当てることができません。

1. ff00:0:0:0:0:0:0:0
2. ff01:0:0:0:0:0:0:0
3. ff02:0:0:0:0:0:0:0
4. ff03:0:0:0:0:0:0:0
5. ff04:0:0:0:0:0:0:0
6. ff05:0:0:0:0:0:0:0
7. ff06:0:0:0:0:0:0:0
8. ff07:0:0:0:0:0:0:0
9. ff08:0:0:0:0:0:0:0

10. ff09:0:0:0:0:0:0:0
11. ff0a:0:0:0:0:0:0:0
12. ff0b:0:0:0:0:0:0:0
13. ff0c:0:0:0:0:0:0:0
14. ff0d:0:0:0:0:0:0:0
15. ff0e:0:0:0:0:0:0:0
16. ff0f:0:0:0:0:0:0:0

（2） 全ノードアドレス

全ノードアドレスは，指定されたスコープ内すべての IPv6 ノードの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは指定スコープ内すべてのノードで受信されます。全ノードアドレスの種類を次に示します。

1. ff01:0:0:0:0:0:0:1 ノードローカル・全ノードアドレス
2. ff02:0:0:0:0:0:0:1 リンクローカル・全ノードアドレス

（3） 全ルータアドレス

全ルータアドレスは，指定されたスコープ内すべての IPv6 ルータの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは指定スコープ内すべてのルータで受信されます。全ルータアドレスの種類を次に示します。

1. ff01:0:0:0:0:0:0:2 ノードローカル・全ルータアドレス
2. ff02:0:0:0:0:0:0:2 リンクローカル・全ルータアドレス
3. ff05:0:0:0:0:0:0:2 サイトローカル・全ルータアドレス

（4） 要請ノードアドレス

要請ノードアドレスは，ノードのユニキャストアドレスとエニキャストアドレスから変換され，要請ノードのアドレス（ユニキャスト，またはエニキャスト）の下位 24 ビットを 104 ビットのプレフィックス ff02:0:0:0:0:1:ff00::/104 に加えたものです。要請ノードアドレスの範囲を次に示します。

ff02:0:0:0:0:1:ff00:0000　～　ff02:0:0:0:0:1:ffff:ffff

集約プロバイダごとに上位プレフィックスが異なるなどの理由で上位の数ビットだけが異なる IPv6 アドレスが生成された場合，これらのアドレスは同じ要請ノードアドレスとなります。これによってノードが加入しなくてはならないマルチキャストアドレスの数を少なくできます。

16.2.6　IPv6 アドレス付与単位

本装置でアドレスを付与する単位をインタフェースと呼びます。最も基本的な接続形態では，一つの物理回線に対して一つのインタフェースを設定します。IPv6 では一つのインタフェースに複数の IPv6 アドレスを設定することができ，IPv6 アドレスを設定したインタフェースには自動的に IPv6 リンクローカルアドレスが付与されます。ただし，リンクローカルアドレスをコンフィグレーションで設定した場合を除きます。ネットワークへの接続形態については，「11.2.1　IP アドレス付与単位」を参照してください。

IPv6 アドレス設定時のネットワークへの接続形態を次の表に示します。

表 16-3 IPv6 アドレス設定時のネットワークへの接続形態

メディア種別	ネットワークへの接続形態		デフォルト値
	ブロードキャスト型	ポイント - ポイント型	
イーサネット	○	-	-
トンネル	-	○	-

（凡例） ○：サポートする -：該当しない

16.2.7 本装置で使用する IPv6 アドレスの扱い

(1) 設定できるアドレス

本装置のインタフェースに付与する IPv6 アドレスとして次のアドレスを使用できます。

1. グローバルユニキャストアドレス
2. リンクローカルユニキャストアドレス

また，次に示す IPv6 アドレスは設定できますが，グローバルユニキャストアドレスと同等として扱われます。

1. サイトローカルユニキャストアドレス
2. エニキャストアドレス
3. アドレスフォーマットプレフィックスが未割り当てのユニキャストアドレス
4. NSAP 互換アドレス
5. IPX 互換アドレス

(2) 設定できないアドレス

次に示す形式の IPv6 アドレスはインタフェースに付与することはできません。

1. マルチキャストアドレス
2. 未定義アドレス
3. ループバックアドレス
4. IPv4 互換アドレス
5. IPv4 射影アドレス
6. 上位 10 ビットが 1111 1110 10 で始まり，11 ビットから 64 ビットまでがすべて 0 ではないアドレス
7. 上位 10 ビットが 1111 1111 10 で始まり，以降のビットがすべて 0 のアドレス
8. プレフィックス長が 64 以外の時に，インタフェース ID 部がすべて 0 となるアドレス

(3) インタフェース ID 省略時のアドレス自動生成

本装置では，インタフェースへの IPv6 アドレス設定時に，インタフェース ID を省略したプレフィックス形式を指定できます。プレフィックス形式指定の場合，プレフィックス長が 64，または省略した形式で指定すると，インタフェース ID を装置側で MAC アドレスや PPP のインタフェース ID から自動生成できます。アドレス自動生成例を次の図に示します。

図 16-17　アドレス自動生成例

1.	アドレスプレフィックス 3ffe:0501:0811:ff01	インタフェースID 0000:0000:0000:0000
		＋
2.		インタフェースID自動生成 0200:87ff:fed0:3090
		↓
3.	アドレスプレフィックス 3ffe:0501:0811:ff01	インタフェースID 0200:87ff:fed0:3090

1.アドレスプレフィックス形式を指定する。(例 3ffe:0501:0811:ff01::)
2.インタフェースIDをメディア種別によって自動生成する。(例 0200:87ff:fed0:3090)
3.生成されたインタフェースIDと指定されたアドレスプレフィックスを合成してアドレスとする。

また，インタフェースにリンクローカルアドレス以外の IPv6 アドレスが指定されたときに該当するインタフェースにリンクローカルアドレスが存在しなかった場合は，自動的にリンクローカルユニキャストアドレスを生成し設定します。さらに，インタフェースに対してリンクローカルユニキャストアドレスだけを自動生成で設定することもできます。

(4) プレフィックス長で設定できる条件

本装置では，インタフェース ID の指定がない場合は自動生成を行います。インタフェース ID の長さは 64 ビット固定となっているため，プレフィックス長で 64 または省略以外の指定が行われた場合は，インタフェース ID を自動生成しないで，入力されたプレフィックスをアドレスとして判断します。そのため下位 64 ビットがすべて 0 になるようなアドレス指定は設定できません。プレフィックス長で設定できる条件を次の表に示します。

表 16-4　プレフィックス長で設定できる条件

アドレス指定形式	設定許可	説明
3ffe:501::/1 ～ 3ffe:501::/31	○	プレフィックス長の指定がプレフィックスより短いため，インタフェース ID 部がすべて 0 にはならないので設定できます。
3ffe:501::/32 ～ 3ffe:501::/63	×	プレフィックス長の指定がプレフィックスより長いため，インタフェース ID 部がすべて 0 になるので設定できません。
3ffe:501::/64 or 3ffe:501::	○	プレフィックス長が 64 または未指定でインタフェース ID 部が省略されている場合はインタフェース ID を装置で自動生成するため設定できます。
3ffe:501::/65 ～ 3ffe:501::/128	×	プレフィックス長の指定がプレフィックスより長いため，インタフェース ID 部がすべて 0 になるので設定できません。

(凡例)　○ : 設定できる　× : 設定できない

16.2.8　ステートレスアドレス自動設定機能

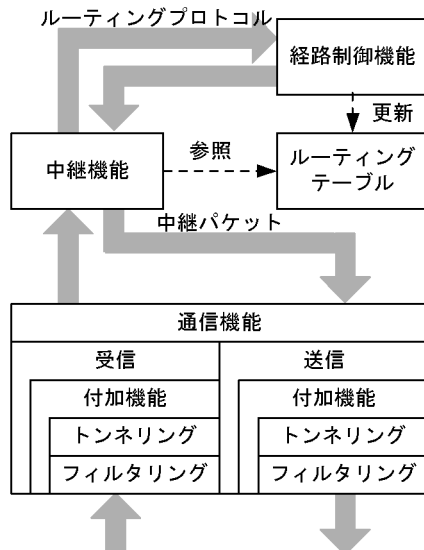
IPv6 リンクローカルアドレスを装置内で自動生成する機能，およびホストが IPv6 アドレスを自動生成する場合に必要な情報をルータから通知する機能です。本装置では IPv6 ステートレスアドレス自動設定 (RFC2462 準拠) をサポートしています。

16.2.9　ホスト名情報

本装置では，IPv4 と同様に，ネットワーク上の装置を識別するためにホスト名情報を定義できます。設定方法については，「解説書 Vol.2　14.1.3 ホスト名情報」を参照してください。コンフィグレーションコマンド hosts，または DNS リゾルバ機能を使用して，IPv4 と IPv6 で同一のホスト名が設定されている場合，IPv4 が優先されます。

16.3　IPv6 レイヤ機能

本装置は受信した IPv6 パケットをルーティングテーブルに従って中継します。この中継処理は大きく分けて次の四つの機能から構成されています。次の図に IPv6 ルーティング機能の概略構成図を示します。

図 16-18　IPv6 ルーティング機能の概略構成図

- 通信機能
  IPv6 レイヤの送信および受信処理を行う機能です。
- 中継機能
  ルーティングテーブルに従って IPv6 パケットを中継する機能です。
- 経路制御機能
  経路情報の送受信や，中継経路を決定してルーティングテーブルを作成する機能です。
- 付加機能
  フィルタリング機能，およびトンネル機能をサポートします。フィルタリングは特定のパケットを中継または廃棄する機能です。フィルタリングは送信と受信の両方の契機で行うことができます。トンネリングは IPv4 ネットワーク上で IPv6 通信を，また IPv6 ネットワーク上で IPv4 通信を実現する機能です。

16.4　通信機能

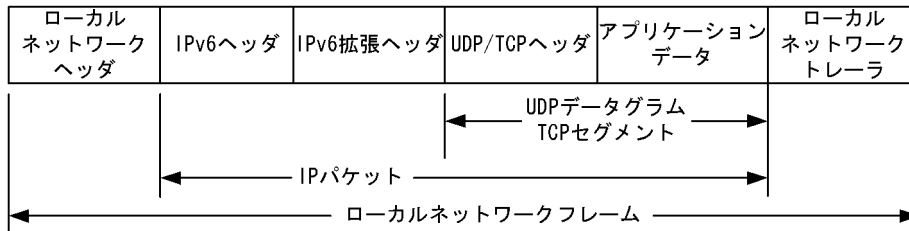
この節では IPv6 で使用する通信プロトコルについて説明します。IPv6 で使用する通信プロトコルには次に示すものがあります。

- IPv6
- ICMPv6
- NDP

16.4.1　インターネットプロトコル　バージョン 6 (IPv6)

(1) IPv6 パケットフォーマット

本装置が送信する IPv6 パケットのフォーマットおよび設定値は RFC2460 に従います。IPv6 パケットフォーマットを次の図に示します。

図 16-19　IPv6 パケットフォーマット

本装置がサポートする IPv6 拡張ヘッダについては「(3) IPv6 拡張ヘッダサポート仕様」を参照してください。

(2) IPv6 パケットヘッダ有効性チェック

IPv6 では 40 オクテット長のヘッダに，8 個のフィールドと 2 個のアドレスが含まれます。IPv6 ヘッダ形式を次の図に示します。

図 16-20　IPv6 ヘッダ形式

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

バージョン	トラフィッククラス	フローラベル	
ペイロード長		次ヘッダ	ホップリミット
始点アドレス			
終点アドレス			

・バージョン(4ビット)　IPバージョンを示す領域
・トラフィッククラス(8ビット)　クラス，優先度の特定および識別
・フローラベル(20ビット)　パケットの属するフローの番号
・ペイロード長(16ビット)　オクテット単位で示したペイロード長
・次ヘッダ(8ビット)　IPv6ヘッダ直後に続くヘッダの種別
・ホップリミット(8ビット)　中継限界数
・始点アドレス(128ビット)　パケットの送信元アドレス
・終点アドレス(128ビット)　パケットの宛先アドレス

IPv6 パケット受信時に IPv6 パケットヘッダの有効性チェックを行います。IPv6 パケットヘッダのチェック内容を次の表に示します。

表 16-5　IPv6 パケットヘッダのチェック内容

IPv6 パケット ヘッダフィールド	チェック内容	チェック NG 時 パケット処理	パケット廃棄時 ICMPv6 送信
バージョン	バージョン＝ 6 であること	廃棄する	送出しない
トラフィッククラス	チェックしない	-	-
フローラベル	チェックしない	-	-
ペイロード長	パケット長と比較する パケット長＜ペイロード長	廃棄する	送出しない
	パケット長と比較する パケット長≧ペイロード長	パケットの後部をペイロード長で削除する	送出しない
次ヘッダ	チェックしない	-	-
ホップリミット	自装置宛てアドレスの受信パケットのホップリミットチェックしない	-	-
	フォワーディングするパケットのホップリミット ホップリミット -1 ＞ 0 であること	廃棄する	送出する※
送信元アドレス	次の条件を満たすこと 1. リンクローカルアドレスでないこと 2. マルチキャストアドレスでないこと	廃棄する	送出しない
宛先アドレス	次の条件を満たすこと 1. ループバックアドレスでないこと 2. インタフェース ID 部が 0 でないこと（ただし，未定義アドレスを除く）	廃棄する	送出しない

（凡例） - : 該当しない

注※ ICMPv6 Time Exceeded メッセージを送信します。

（3） IPv6 拡張ヘッダサポート仕様

本装置がサポートする IPv6 拡張ヘッダの項目を次の表に示します。

表 16-6 IPv6 拡張ヘッダの項目

IPv6 拡張ヘッダ	IPv6 パケットの分類		
	本装置が発局となるパケット	本装置が着局となるパケット※1	本装置が中継するパケット
Hop-by-Hop Options Header	○	○	○※2
Routing Header	○	○	-
Fragment Header	○	○	-
Authentication Header	×	×	-
Encapsulating Security Payload Header	×	×	-
Destination Options Header	○	○	-

（凡例） ○ : サポートする × : サポートしない - : ヘッダ処理なし

注※ 1

本装置が着信するパケットが次の条件に該当する場合，パケットは廃棄されます。

- 拡張ヘッダが 9 個以上設定されたパケット
- 一つの拡張ヘッダ内に 9 個以上のオプションが設定されたパケット

注※ 2

本装置が中継するパケットが次の条件に該当する場合，パケットは廃棄されます。

- Hop-by-Hop Options ヘッダ内に 9 個以上のオプションが設定されたパケット

16.4.2 ICMPv6

本装置が送信する ICMPv6 メッセージのフォーマットおよび設定値は RFC2463 に従います。ICMPv6 メッセージのサポート仕様を次の表に示します。

表 16-7 ICMPv6 メッセージサポート仕様

ICMPv6 メッセージ				サポート
タイプ (種別)	値 (10 進)	コード (詳細種別)	値 (10 進)	
DestinationUnreachable	1	no route to destination	0	○
		communication with destination administratively prohibited	1	○
		beyond scope of source address	2	×
		address unreachable	3	○
		port unreachable	4	○
Packet Too Big	2	-	0	○
Time Exceeded	3	hop limit exceeded in transit	0	○
		fragment reassembly time exceeded	1	○

ICMPv6 メッセージ				サポート
タイプ (種別)	値 (10 進)	コード (詳細種別)	値 (10 進)	
Parameter Problem	4	erroneous header field encountered	0	○
		unrecognized Next Header type encountered	1	○
		unrecognized IPv6 option encountered	2	○
Echo Request	128	-	0	○
Echo Reply	129	-	0	○
Multicast Listener Query	130	-	0	○
Multicast Listener Report	131	-	0	○
Multicast Listener Done	132	-	0	○
Router Solicitation	133	-	0	○
Router Advertisement	134	-	0	○
Neighbor Solicitation	135	-	0	○
Neighbor Advertisement	136	-	0	○
Redirect	137	-	0	○

(凡例) ○：サポートする　×：サポートしていない　-：該当しない

(1) ICMPv6 Redirect の送信仕様

次の条件を満たすときに ICMPv6 Redirect のパケットを送信します。

- パケット送信元とネクストホップのルータが同一リンク内にある
- 受信パケットが ICMPv6 以外の IPv6 パケット

(2) ICMPv6 Time Exceeded の送信仕様

次の条件を満たすときに ICMPv6 Time Exceeded のパケットを送信します。

- フォワーディングする受信 IPv6 パケットの Hoplimit が 1 の場合
- 受信パケットが ICMPv6 以外の IPv6 パケット

16.4.3 NDP

本装置が送信する NDP フレームのフォーマット，および設定値は RFC2461 に従います。

(1) ProxyNDP

本装置はイーサネットに接続するすべてのインタフェースで ProxyNDP を動作させることができます。動作させるかどうかはコンフィグレーションで設定します。本装置は次の条件をすべて満たす NDP 近隣要求メッセージを受信した場合に，宛先プロトコルアドレスの代理として NDP 近隣広告メッセージを送信します。

- NDP 近隣要求メッセージの宛先プロトコルアドレスがマルチキャストアドレス，エニキャストアドレスではない
- NDP 近隣要求メッセージの送信元プロトコルアドレスと宛先プロトコルアドレスのネットワーク番号が等しい

- NDP 近隣要求メッセージの宛先プロトコルアドレスがルーティングテーブルにあり到達できる

（2） NDP エントリの削除条件

次の条件のどれかを満たす場合，該当する NDP エントリを削除します。ただし，コンフィグレーションで定義されたスタティック NDP エントリは削除しません。

- NDP エントリに対応する IPv6 アドレスとの通信が停止した後，10 分が経過した場合
- ステータス状態が stale の NDP エントリに対応する IPv6 アドレスへ通信が再開された時に到達性がなかった場合
- インタフェース状態が Down となった場合の該当するインタフェースに存在する全 NDP エントリ

（3） スタティック NDP 情報の設定

NDP プロトコルを持たない製品を接続するために，イーサネットの MAC アドレスと IPv6 アドレスの対応（スタティック NDP 情報）をコンフィグレーションで設定できます。

（4） NDP 情報の参照

運用端末からコマンドで NDP 情報が参照できます。NDP 情報から該当するインタフェースの IPv6 アドレスと MAC アドレスの対応がわかります。

16.5　中継機能

中継機能とは，受信したパケットをルーティングテーブルに従って次のルータまたはホストに転送する処理機能です。

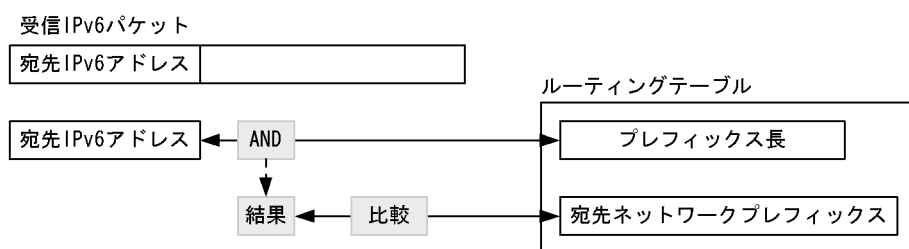
16.5.1　ルーティングテーブルの内容

ルーティングテーブルは複数個のエントリから構成されており，各エントリは次の内容を含んでいます。本装置のルーティングテーブルの内容はコマンドで表示できます。

- Destination：
  宛先ネットワークプレフィックス，アドレスとそのプレフィックス長。プレフィックス長は，ルーティングテーブル検索時，受信 IPv6 パケットの宛先アドレスに対するマスクとなります。なお，ホストアドレスによる中継を行う場合には 128 を表示します。
- Next Hop：次に中継するルータの IPv6 アドレス
- Interface：Next Hop のあるインタフェース名称
- Metric　：ルートのメトリック
- Protocol ：学習元プロトコル
- Age　　：ルートが確認，または変更されてからの時間 (秒)

16.5.2　ルーティングテーブルの検索

受信した IPv6 パケットの宛先アドレスに該当するエントリをルーティングテーブルから検索します。該当するエントリとは，受信した IPv6 パケットの宛先アドレスを各エントリのプレフィックス長で上位ビットよりマスク (AND) を取り，その結果が宛先ネットワークプレフィックスと同じ値になるものです。ルーティングテーブルの検索を次の図に示します。

図 16-21　ルーティングテーブルの検索

16.6　フィルタリング

フィルタリング機能は，受信したある特定の IPv6 パケットを中継または廃棄できます。フィルタリング機能の詳細については「11.6　フィルタリング」を参照してください。

16.6.1　フロー検出条件

フロー検出条件を次の表に示します。

表 16-8　フロー検出条件

ヘッダ種別	設定項目	項目設定
MAC	送信元 MAC アドレス※	MAC アドレスを単一指定，またはマスク指定できます。
	宛先 MAC アドレス※	MAC アドレスを単一指定，またはマスク指定できます。
	イーサネットタイプ※	IPv4，IPv6，IPX などのプロトコル種別を指定します。
	ユニキャストフラッディングフレーム識別子※	フラッディングされたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出します。出力側だけ指定できます。
Tag-VLAN	VLAN ID ※	VLAN 番号
	ユーザ優先度	優先度情報
IP	IP ユーザデータ長	IP ユーザデータの上限値または下限値
	上位プロトコル	TCP，UDP などを示す番号
	送信元 IP アドレス	アドレスを単一指定，範囲指定，またはサブネット指定できます。
	宛先 IP アドレス	アドレスを単一指定，範囲指定，またはサブネット指定できます。
	DSCP	トラフィッククラスフィールドの上位 6 ビット
	プレシデンス	トラフィッククラスフィールドの上位 3 ビット
TCP	送信元ポート番号	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	宛先ポート番号を単一指定，または範囲指定できます。
	ACK フラグ	ACK フラグが 1 のパケットを検出します。
	SYN フラグ	SYN フラグが 1 のパケットを検出します。
UDP	送信元ポート番号	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	宛先ポート番号を単一指定，または範囲指定できます。
ICMPv6	ICMPv6 タイプ	Echo Request/Echo Reply/Destination Unreachable などを示す番号
	ICMPv6 コード	不明な IPv6 オプションなどの ICMPv6 タイプに対する詳細コードを示す番号

注※

出力側のインタフェースで，送信元 MAC アドレス，宛先 MAC アドレス，イーサネットタイプ，および VLAN ID で IPv4，IPv6 中継パケットを検出することはできません。

本装置は，イーサネットタイプとしてイーサネット V2 形式と，IEEE802.3 の SNAP/RFC1042 形式のイーサネットフレームのイーサネットタイプを検出できます。イーサネットタイプの位置を次の図に示します。

図 16-22　イーサネットタイプの位置

イーサネットV2形式

宛先MAC アドレス	送信元MAC アドレス	イーサネット タイプ	データ	FCS

IEEE802.3 SNAP/RFC1042形式

宛先MAC アドレス	送信元MAC アドレス	長さ	DSAP= 0xAA	SSAP= 0xAA	制御= 0x03	SNAP OUI =0x000000	イーサネット タイプ	データ	FCS

ユニキャストフラッディングフレーム識別子 (unicast_flood) は，本装置がフラッディングしたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出するための条件です。フラッディングとは，フレームを受信した物理ポートを除く同一 VLAN 内の全ポートへ，フレームを転送する動作です。

16.6.2　IPv6 DHCP サーバ機能との連携

本機能は，IPv6 DHCP サーバ機能でのプレフィックスの配布と連携し，配布したプレフィックスを送信元 IPv6 アドレス，または宛先 IPv6 アドレスとするパケットを中継する機能です。配布していないプレフィックスを使用した不正なパケットは廃棄します。

本機能を使用するには，コンフィグレーション dhcp6_server を設定後，IPv6 フィルタの送信元 IPv6 アドレス，または宛先 IPv6 アドレスに pd_prefix を指定します。

16.6.3　フィルタリングの運用について

フィルタリングでは，フロー検出条件モードおよびフロー検出条件オプションで運用方法を選択できます。

(1)　フロー検出条件モード

フロー検出条件モードでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法は QoS 制御も同じ運用法となります。

表 16-9　フロー検出条件モードで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件モードの指定方法
1	きめ細かいフロー検出条件を指定する	MAC，IP ヘッダなどを検出条件としてパケット検出が可能。	フロー検出条件モードの指定なし
2	パケット中継性能を劣化させない	<Portlist> 指定では，L2 スイッチ中継を対象とし，<Interface Name> 指定では，IPv4，IPv6 中継パケットを対象としたパケット検出が可能。	フロー検出条件モード 1 (retrieval_mode_1) を指定

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 16-10　フロー検出条件モードと対応可能 PSU，BSU の関係

フロー検出条件モード	対応可能 PSU	対応可能 BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2
フロー検出条件モード 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a) フロー検出条件モード 1

パケット中継性能を劣化させることなく，フィルタリング機能を使用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件モード 1 を指定します。

フロー検出条件モード 1 を有効とするには，指定 PSU に「表 16-10　フロー検出条件モードと対応可能 PSU，BSU の関係」で示す対応可能 PSU を実装してください。フロー検出条件モード 1 をサポートしていない PSU に対してフロー検出条件モード 1 を設定した場合，フローフィルタ機能，フロー QoS 機能は動作しません。

フロー検出条件モード 1 指定時，設定した入出力インタフェースごと (<Portlist> 指定，または <Interface Name> 指定) に指定可能なフロー検出条件を「表 16-11　フロー検出条件モード 1 時のフロー検出条件」に示します。

なお，QoS 制御もフロー検出条件モード 1 で動作します。フロー検出条件モード 1 指定時，QoS 制御で指定可能なフロー検出条件は，「解説書 Vol.2　1.3.1 フロー検出機能の運用について」を参照してください。

表 16-11　フロー検出条件モード 1 時のフロー検出条件

ヘッダ種別	設定項目	<Portlist> 指定	<Interface Name> 指定
MAC	送信元 MAC アドレス	○	-
	宛先 MAC アドレス	○	-
	イーサネットタイプ	○	-
	ユニキャストフラッディングフレーム識別子	○※	-
Tag-VLAN	VLAN ID	○	-
	ユーザ優先度	○	○
IP	IP ユーザデータ長	-	○
	上位プロトコル	-	○
	送信元 IP アドレス	-	○
	宛先 IP アドレス	-	○
	DSCP	○	○
	プレシデンス	○	○
TCP	送信元ポート番号	-	○
	宛先ポート番号	-	○
	ACK フラグ	-	○

ヘッダ種別	設定項目	<Portlist> 指定	<Interface Name> 指定
	SYN フラグ	-	○
UDP	送信元ポート番号	-	○
	宛先ポート番号	-	○
ICMPv6	ICMPv6 タイプ	-	○
	ICMPv6 コード	-	○

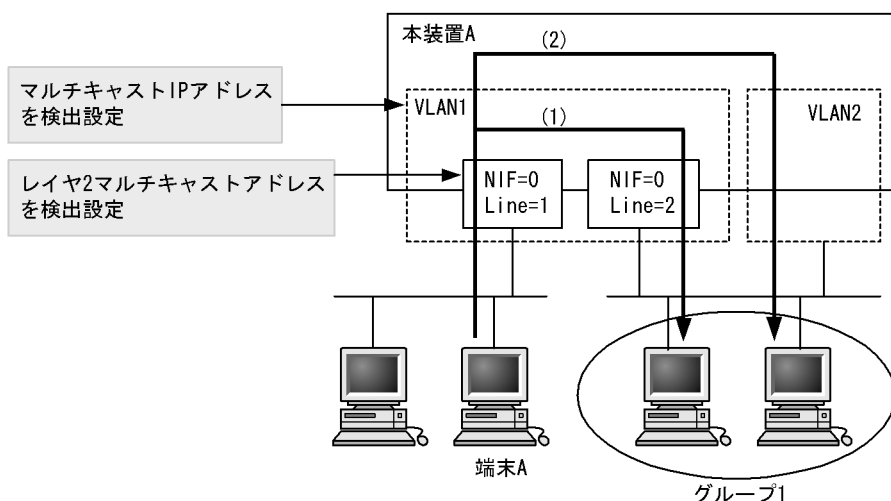
(凡例) ○ : 指定可 - : 指定不可
注※ 出力側だけ指定可能です。

次にフロー検出条件モード 1 を使用した場合の <Portlist> 指定，<Interface Name> 指定ごとの検出可能なパケットを示します。

表 16-12 検出可能パケット種別一覧

フロー指定方法	パケット種別
<Portlist> 指定	レイヤ 2 スイッチ中継パケット※
<Interface Name> 指定	IPv4，IPv6 中継パケット※

注※
宛先 MAC アドレスがレイヤ 2 マルチキャストアドレス，かつ宛先 IP アドレスがマルチキャスト IP アドレスのパケットは，本装置でレイヤ 2 スイッチ中継および IPv4，IPv6 中継の両方を実施します (次に示す図の (1)，(2))。したがって，コンフィグレーションコマンド flow filter で，(1) のレイヤ 2 スイッチ中継パケットをフィルタリングする場合は，<Portlist> 指定で宛先 MAC アドレス検出条件にレイヤ 2 マルチキャストアドレスを指定して，(2) の IPv4，IPv6 中継パケットをフィルタリングする場合は <Interface Name> 指定で，宛先 IPv6 アドレス検出条件にマルチキャスト IP アドレスを指定してください。

図 16-23 マルチキャストパケット中継例

(2) フロー検出条件オプション

フロー検出条件オプションでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法は QoS 制御も同じ運用方法となります。

表 16-13　フロー検出条件オプションで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件オプションの指定方法
1	中継パケットでフロー検出する	中継パケットでだけフロー検出可能	フロー検出条件オプションの指定なし
2	中継パケットおよび本装置宛パケット※でフロー検出したい	中継パケットおよび本装置宛パケット※でフロー検出可能	フロー検出条件オプション 1 (retrieval_option_1) を指定

注※

フロー検出条件オプション 1 指定時にフロー検出対象に加わる本装置宛パケットは次に示すパケットです。したがって，フロー検出条件オプション 1 を指定しない場合，次に示す本装置宛パケットはフロー検出対象外です。

- 宛先 MAC アドレスがブロードキャストアドレスであるパケット
- 宛先 MAC アドレスがマルチキャスト MAC アドレスまたは自 MAC アドレスである非 IP パケット
- 送信元 IP アドレスまたは宛先 IP アドレスがリンクローカルアドレスであるパケット

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 16-14　フロー検出条件オプションと対応可能 PSU，BSU の関係

フロー検出条件オプション	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2
フロー検出条件オプション 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a) フロー検出条件オプション 1

本装置宛パケット（表 16-13　フロー検出条件オプションで選択できる運用方法の注参照）でもフロー検出機能を運用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件オプション 1 を指定します。フロー検出条件オプション 1 を使用する場合は，対象 PSU，対象 BSU に「表 16-14　フロー検出条件オプションと対応可能 PSU，BSU の関係」で示す対応可能な PSU，BSU を実装してください。なお，QoS 制御もフロー検出条件オプション 1 で動作します。また，フロー検出条件オプション 1 の指定は，フロー検出条件モードと同時に設定できます。

注

EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出するコンフィグレーション flow filter の設定は，次のインタフェースまたは物理ポートに指定してください。

- Tag-VLAN 連携回線の untagged の論理インタフェース
- VLAN 回線の untagged ポートが属する VLAN インタフェース

16.6.4　フロー検出とパケット中継方式との対応

パケット中継方式によってフロー検出可能なパケットが異なります。パケット中継方式との対応を，次の「表 16-15　パケット中継方式との対応」に示します。

表 16-15　パケット中継方式との対応

フロー検出		レイヤ 2 スイッチ中継		IPv6 中継	
		受信側	送信側	受信側	送信側
MAC ヘッダ	送信元 MAC アドレス	○	○	○	○※ 1
	宛先 MAC アドレス	○	○	○	○※ 1
	イーサネットタイプ	○	○	○	-
Tag-VLAN ヘッダ	ユーザ優先度	○	○※ 2	○	○※ 3
	VLAN ID	○	○	○	○※ 4
IP ヘッダ※ 5		○	○	○	○
レイヤ 4 ヘッダ (TCP/UDP など)※ 5		○	○	○※ 6 ※ 7	○※ 6 ※ 7

(凡例)　○：サポート　　-：未サポート

注※ 1

特定の MAC アドレスのフロー検出は未サポートです。すべての MAC アドレスをフロー検出すること (コンフィグレーションコマンド flow filter での MAC アドレスに any と指定) ができます。

注※ 2

レイヤ 2 スイッチ中継で，送信側でのユーザ優先度で検出を指定したときは，次のようになります。

- 受信側で VLAN-Tag 無しフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。
- 受信側で VLAN-Tag 付きフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，受信時のユーザ優先度で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※ 3

IPv4 中継で，送信側でユーザ優先度のフロー検出を指定したときは，次のようになります。

- 受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
- 受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※ 4

インタフェース名指定で，Tag-VLAN 連携回線の場合，VLAN ID でフロー検出可能です。この場合，VLAN ID をフロー検出条件として指定する必要はありません。Tag-VLAN 連携回線以外のインタフェースおよび物理ポートでは，未サポートです。

注※ 5

Tag-VLAN ヘッダが 2 個までの場合です。3 個以上の場合は未サポートです。

注※ 6

2 番目以降のフラグメントパケットを 4 層 (TCP，UDP，ICMP，IGMP) のフロー検出条件にてフィルタリングを実施した場合，2 番目以降のフラグメントパケットはレイヤ 4 ヘッダがパケット内にないため，同じフロー検出条件で検出できません。フラグメントパケットを含めたフィルタリングを実施する場合は，フロー検出条件に 3 層ヘッダ条件を指定するようにしてください。

注※ 7

暗号ペイロードオプションまたは認証オプションが付加されているパケットは未サポートです。また，暗号ペイロードオプションまたは認証オプション以外の拡張ヘッダ付きパケットの場合は，本装置で「パケットのレイヤ 4 ヘッダが見える，見えない」でソフトウェア中継，ハードウェア中継が選択されます。詳細は，「16.6.5　フィルタリング使用時の注意事項」を参照してください。

16.6.5 フィルタリング使用時の注意事項

(1) フラグメントパケットをフロー検出する場合の注意事項

2 番目以降のフラグメントパケットを 4 層 (TCP,UDP,ICMP,IGMP) のフロー検出条件でフィルタリングを実施した場合，2 番目以降のフラグメントパケットはレイヤ 4 ヘッダがパケット内にないため，同じフロー検出条件で検出できません。フラグメントパケットを含めたフィルタリングを実施する場合は，フロー検出条件に 3 層ヘッダ条件を指定するようにしてください。

なお，先頭フラグメントパケットを中継した場合，2 番目以降のフラグメントパケットを常に中継します。

(2) レイヤ 4 ヘッダ検出条件でフロー検出する場合の注意事項

1. 暗号ペイロードオプションまたは認証オプションが付加されているパケットを受信した場合，ポート番号などのレイヤ 4 ヘッダ条件で検出することはできません。
2. 暗号ペイロードオプションまたは認証オプション以外の拡張ヘッダ付きパケットや，拡張ヘッダがないパケットを受信し，フィルタリングのフロー検出条件としてポート番号などのレイヤ 4 ヘッダ検出条件を設定している場合：
    1. パケットのレイヤ 4 ヘッダが見えるとき (次の表を参照してください)
       ハードウェア処理によってフィルタリングを実行します。
    2. パケットのレイヤ 4 ヘッダが見えないとき (次の表を参照してください)
       レイヤ 3 中継の場合は，ソフトウェア処理によってフィルタリングを実行します。レイヤ 2 スイッチ中継の場合は，フィルタリングで指定した動作を行わず，受信ッパケットを中継します。

表 16-16 受信側でのレイヤ 4 ヘッダ判別可否パターン

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
IPv6 拡張ヘッダなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv6 拡張ヘッダあり (拡張ヘッダ 8byte 以下)	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv6 拡張ヘッダあり	POS【SB-7800S】		×	×

受信パケット			レイヤ4ヘッダ内のフィールド	
レイヤ3ヘッダ	レイヤ2ヘッダ		TCP/UDP※1 ICMP/IGMP※2	TCP CODEBIT
(拡張ヘッダ 9byte 以上)	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

（凡例） ○：該当フィールドの検出可　×：該当フィールドの検出不可

注※1　：送信元ポート番号 , 宛先ポート番号

注※2　：Type,Code

表 16-17　送信側でのレイヤ4ヘッダ判別可否パターン

送信パケット			レイヤ4ヘッダ内のフィールド	
レイヤ3ヘッダ	レイヤ2ヘッダ		TCP/UDP※1 ICMP/IGMP※2	TCP CODEBIT
IPv6 拡張ヘッダなし	POS【**SB-7800S**】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	×
IPv6 拡張ヘッダあり (拡張ヘッダ 8byte 以下)	POS【**SB-7800S**】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	×
	IEEE802.3	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	×	×
IPv6 拡張ヘッダあり (拡張ヘッダ 9byte 以上)	POS【**SB-7800S**】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
		Tag 付き (Tag 数 2)	×	×

（凡例） ○：該当フィールドの検出可　×：該当フィールドの検出不可
注※ 1　：送信元ポート番号 , 宛先ポート番号
注※ 2　：Type,Code

(3) プライベート VLAN 使用時の注意事項

プライベート VLAN 機能を使用している VLAN に対するフィルタリング機能は，該当 VLAN の物理ポート (<Portlist> 指定) に対する設定だけサポートしています。該当 VLAN のインタフェース (<Interface Name> 指定) に対する設定は未サポートです。

(4) show filter-flow 運用コマンドのフローフィルタ統計情報の表示について

1. 下記条件を満たすコンフィグレーション flow filter を指定した物理ポートまたはインタフェースが，show vlan コマンドでの Port Information の表示において Blocking 状態の場合，廃棄したパケットのフローフィルタ統計情報は採取されません。
   - 条件 1
     フロー検出条件オプション 1 を指定
   - 条件 2
     コンフィグレーション flow filter で EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出し，廃棄動作指定を設定
2. フロー検出条件オプション 1 の指定時， 1 物理ポートだけ指定した VLAN 回線で，宛先 MAC アドレスが MAC ブロードキャストのパケットをフロー検出して forward 動作指定を指定した場合，フローフィルタ統計情報は採取されません。

16.6.6 FDB のスタティックエントリ登録機能との併用時の動作

MAC アドレスをフローの検出条件としてパケットの廃棄が可能となる機能として，フィルタリング機能と FDB のスタティックエントリ登録機能の二つがあります。次の表にフィルタリング機能と FDB のスタティックエントリ登録機能とを併用した場合のパケットの廃棄動作について示します。

表 16-18　FDB のスタティックエントリ登録機能との併用時のパケット廃棄動作

フィルタリング機能の動作指定	FDB のスタティックエントリ機能の動作指定	パケットの廃棄動作
中継	中継	-(中継します)
	廃棄	FDB のスタティックエントリ登録機能によってパケットを廃棄します
廃棄	中継	フィルタリング機能によってパケットを廃棄します
	廃棄	フィルタリング機能によってパケットを廃棄します

16.7　ロードバランス

16.7.1　ロードバランス概説

ロードバランスは，マルチパス接続によって IP レイヤのルーティング制御で増大するトラフィックの負荷を分散する機能です。ロードバランスの詳細については「11.7.1　ロードバランス概説」を参照してください。

16.7.2　ロードバランス仕様

本装置で実装するマルチパスの仕様を「表 16-19　IPv6 マルチパス仕様」に，ロードバランスの仕様を「表 16-20　IPv6 ロードバランス仕様」に示します。

デフォルトのコンフィグレーションでは，マルチパスは無効になっています。使用するときは，マルチパスの最大パス数と各ルーティングプロトコルでのマルチパス生成を指定する必要があります。

表 16-19　IPv6 マルチパス仕様

項目	仕様	備考
一宛先ネットワークに対するマルチパス数	2 〜 16 パス	冗長構成の場合，選択するマルチパス数はコンフィグレーションで指定した数になります。
コンフィグレーションのマルチパス数の指定	1 〜 16 1 を指定するとマルチパスを生成しません。	装置単位で指定します。
マルチパスを生成できるルーティングプロトコル	• スタティックルーティング (「17.3.1　スタティックルーティング」参照) • OSPFv3(「17.5.2　経路選択アルゴリズム」参照) • BGP4+(「18.3.8　BGP4+ マルチパス」参照) • IS-IS(「14.2.3　経路選択アルゴリズム」参照)	コンフィグレーションで，各ルーティングプロトコルでマルチパス生成を指定する必要があります。
接続形態	回線種別およびインタフェース種別に関係なく使用できます。また，混在もできます。	-

(凡例)　- : 該当しない

表 16-20　IPv6 ロードバランス仕様

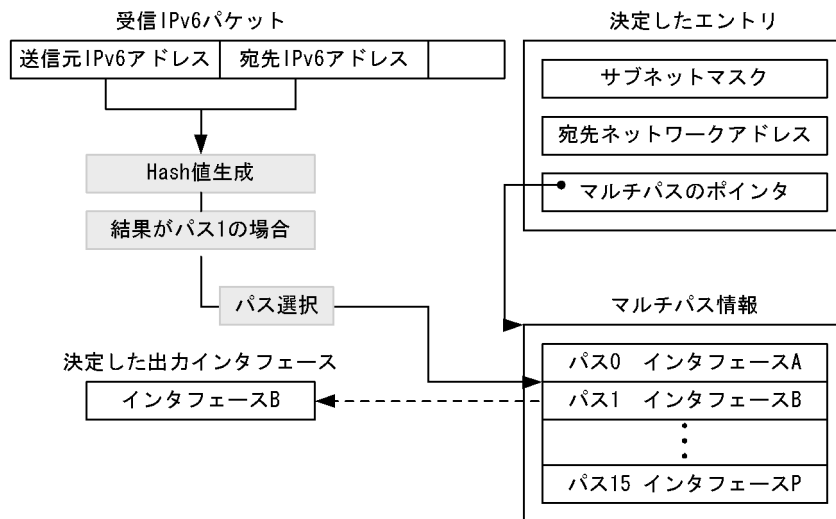
項目	仕様	備考
マルチパスの振り分け方法	宛先 IPv6 アドレスと送信元 IPv6 アドレスから 16 パスに振り分ける値 (Hash 値) を算出し，決定した出力パスに振り分けます。 宛先 IPv6 アドレスと送信元 IPv6 アドレスが同一のパケットは，同一出力パスを選択します。これによって，送信の順序性を保証します。	-
Hash 値	256 通り 宛先 IPv6 アドレスと送信元 IPv6 アドレスから算出します。	-
ルーティングテーブル内のマルチパス情報	ルーティングテーブルに設定する各出力インタフェースの Hash 値の割り当て比率は，ほぼ均等になります。	「16.7.5　ロードバランス使用時の注意事項」の 1 を参照
各パスの重み付け	できません。	

項目	仕様	備考
出力帯域を超えたパケットの処理	別のパスに振り分けません。継続して帯域を超えた場合は，装置内で保持しますが，保持しきれない場合パケットを廃棄します。	

(凡例)- : 該当しない

16.7.3 出力インタフェースの決定

ルーティングテーブルの検索で，宛先 IPv6 アドレスに該当するエントリが決定すると，次に出力インタフェースを決定します。出力インタフェースを決定するには，受信した IPv6 パケットの送信元 IPv6 アドレス (Source IPv6 Address) と宛先 IPv6 アドレス (Destination IPv6 Address) から Hash 値を生成し，それによってマルチパスの候補の一つを選択します。出力インタフェースの決定を次の図に示します。

図 16-24　出力インタフェースの決定

16.7.4 Hash 値の計算方法

Hash 値 $H[2^{7-0}]$($H[2^7]$ は 2^7 ビット，$H[2^0]$ は 2^0 ビット，$H[2^{7-0}]$ は 2^0 から 2^7 までのビット列) は，8 ビットで生成します。

送信元 IPv6 アドレスを $S[2^{127-0}]$，宛先 IPv6 アドレスを $D[2^{127-0}]$ とした場合，Hash 値 $H[2^{7-0}]$ の計算式を，次に示します。

$H[2^{7-0}]$ は，送信元 IPv6 アドレスと宛先 IPv6 アドレスの値を，8 ビットごとに加算した結果の下位 8 ビットをビット逆順にした値です。Hash 値の計算方法を次の図に示します。

図 16-25　Hash 値の計算方法

$H'[2^{7-0}] = S[2^{127-120}] + S[2^{119-112}] + S[2^{111-104}] + S[2^{103-96}] + S[2^{95-88}] + S[2^{87-80}]$
$+ S[2^{79-72}] + S[2^{71-64}] + S[2^{63-56}] + S[2^{55-48}] + S[2^{47-40}] + S[2^{39-32}] + S[2^{31-24}]$
$+ S[2^{23-16}] + S[2^{15-8}] + S[2^{7-0}]$
$+ D[2^{127-120}] + D[2^{119-112}] + D[2^{111-104}] + D[2^{103-96}] + D[2^{95-88}] + D[2^{87-80}] + D[2^{79-72}]$
$+ D[2^{71-64}] + D[2^{63-56}] + D[2^{55-48}] + D[2^{47-40}] + D[2^{39-32}] + D[2^{31-24}] + D[2^{23-16}]$
$+ D[2^{15-8}] + D[2^{7-0}]$　(桁上げは無視)
$H[2^{7-0}] = H'[2^{0-7}]$　(ビットを逆順)

$S[2^{127-0}]$=3FFE::1　$D[2^{127-0}]$=3FFE::2

$S[2^{127-120}]$	$S[2^{119-112}]$		$S[2^{15-8}]$	$S[2^{7-0}]$
3F	FE	…	0	1

$D[2^{127-120}]$	$D[2^{119-112}]$		$D[2^{15-8}]$	$D[2^{7-0}]$
3F	FE	…	0	2

↓ 8 ビットごとに加算（桁上げ無視）

$H'[2^{7-0}]$=0x7D

ビットを逆順にして，$H[2^{7-0}] = H'[2^{0-7}]$ = 0x82 = 130
選択パス = Hash値 × 有効パス数 ÷ 256（小数点以下切り捨て）
= 130 × 4 ÷ 256 = 2（有効パス数を4とした場合）

16.7.5　ロードバランス使用時の注意事項

1. Hash 値によって一意に 16 パスの内 1 パスを選択するため，宛先ネットワークに対するそれぞれのパスのパケット分配比率は必ずしも均等になりません。
2. 各パスに重み付けを付けないため，回線速度が異なる場合は速度に比例した分配は行いません。ただし，イーサネット回線の場合，マルチホーム接続することによって回線速度の速い回線に重み付けできますが，障害の発生を考慮して冗長構成とする必要があります。
3. Hash 値によって選択した該当するパスの出力帯域を超えて，継続的にパケットを送出しようとした場合，パケット廃棄が発生します。別のパスには振り分けません。
4. マルチパスに Null インタフェースを含むことはできません。
5. 本装置から自発送信する場合は , 送信元 IPv6 アドレスを :: として Hash 値を算出します。
6. Traceroute(IPv6) によって，ロードバランスで使用する選択パスを確認する場合，次の注意が必要です。
   - Traceroute(IPv6) を受信した回線の IPv6 アドレスを送信元 IPv6 アドレスとして，応答を返しますが，その回線を使用して応答を返すとは限りません。
   - Traceroute(IPv6) を受信した回線がマルチホーム定義の場合，隣接装置がどのサブネットで送信したのか判断できません。このため，マルチホーム内の 1 アドレスを送信元 IPv6 アドレスとして応答します。

16.8 Null インタフェース

IPv6 は Null インタフェースをサポートします。Null インタフェースの詳細については「11.8　Null インタフェース」を参照してください。なお，IPv6 スタティックルーティングおよび経路制御についての詳細は「17　RIPng/OSPFv3」～「18　BGP4+【OP-BGP】」を参照してください。

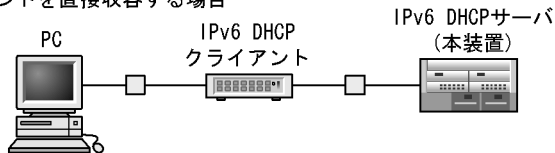
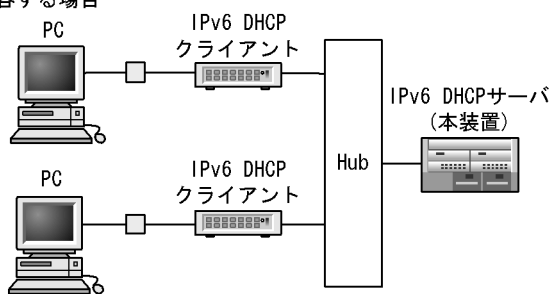
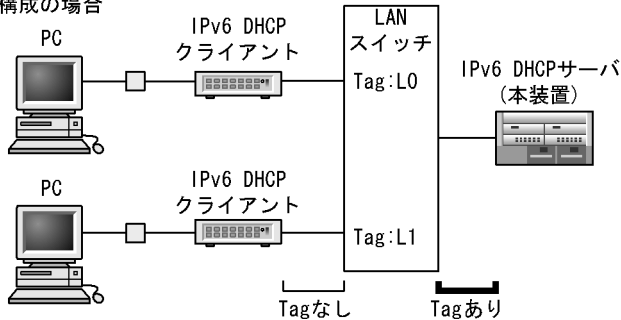
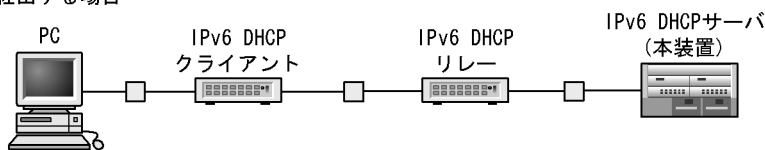
16.9　ポリシールーティング

IPv6 はポリシールーティングをサポートします。ポリシールーティングの詳細については，「11.9　ポリシールーティング」を参照してください。なお，IPv6 フィルタリング機能についての詳細は「16.6　フィルタリング」を参照してください。

16.10 IPv6 DHCP サーバ機能

IPv6 DHCP サーバ機能は，IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

DHCP サーバ機能の接続構成を次の図に示します。

図 16-26 IPv6 DHCP サーバ機能の接続構成

16.10.1 サポート仕様

本装置の DHCP サーバ機能のサポート仕様を次の表に示します。DHCP サーバと DHCP クライアント間の接続は，同一ネットワーク内直結で行います。なお，DHCP サーバが DHCP クライアントに配布できるプレフィックスは SB-7800S の場合最大 8,192 個，SB-5400S の場合最大 1,024 個です。

表 16-21 DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	DHCP クライアント直接収容

項目	仕様
	DHCP リレー経由
サポートメディア	10BASE-T/100BASE-TX
	ギガビット・イーサネット
	10 ギガビット・イーサネット
最大配布 Prefix	• SB-7800S の場合最大 8,192 個 • SB-5400S の場合最大 1,024 個
ネットワーク層プロトコル	IPv6 だけサポート
IPv4/IPv6 デュアルスタック対応	サポート
Tag-VLAN 連携	サポート

16.10.2　サポート DHCP オプション

本装置でサポートする DHCP オプションを次の表に示します。なお，値の設定側の参考として，クライアント側による指定有無についても掲載します。

表 16-22　本装置で対応する DHCPv6 オプション

Option Code	オプション名称	意味	値の設定側	
			クライアント（参考）	本装置（サーバ）
1	Client Identifier	Client Identifier オプションは，クライアントとサーバの間で，クライアントを識別する DUID※1 を運ぶのに使用されます。	○	△
2	Server Identifier	Server Identifier オプションは，クライアントとサーバの間で，サーバを識別している DUID を運ぶのに使用されます。	△	○
3	Identity Association option	Identity Association オプション (IA オプション) は，identity association，IA と関連するパラメータ，IA と関連するアドレスを運ぶのに使用されます。	○／△	-
4	Identity Association for Temporary Addresses option	Temporary Addresses(IA_TA) オプションのための Identity Association は，IA，IA と関連するパラメータ，IA と関連するアドレスを運ぶのに使用されます。RFC 3041 で規定されているように，このオプション中のアドレスすべてが，一時的なアドレスとしてクライアントによって使用されます。	○／△	-
5	IA Address option	IA Address オプションは，IA と関連する IPv6 アドレスを指定するのに使用されます。IA Address オプションは，Identity Association オプションの Options フィールドにカプセル化されなければなりません。Options フィールドは，このアドレスに特有であるそれらのオプションをカプセル化します。	○／△	-
6	Option Request	Option Request オプションは，クライアントとサーバの間で，メッセージの中のオプションのリストを識別するのに使用されます。	○	○
7	Preference	Preference オプションは，クライアントによるサーバの選択に影響を及ぼすために，クライアントにサーバによって送られます。	-	○

Option Code	オプション名称	意味	値の設定側	
			クライアント（参考）	本装置（サーバ）
8	Elapsed Time option	クライアントがどれくらいの間 DHCP メッセージ交換を完了しているかを示すために含めるオプション。経過時間は，メッセージ交換においてクライアントが最初のメッセージを送った時間から測られます。そして，メッセージ交換において最初のメッセージの elapsed-time フィールドは 0 に設定されます。例えば，プライマリ・サーバが合理的な時間で応答しなかったとき，経過時間オプションは，セカンダリ DHCP サーバが要請に応じるのを許可します。	○	-
9	Relay Message option	Relay Message オプションは，Relay-forward または Relay-reply メッセージの中の DHCP メッセージを運びます。	○※2	○
11	Authentication option	Authentication オプションは，DHCP メッセージ識別と内容を認証するために，認証情報を運びます。Authentication オプションの使用法は，セクション 21 で記述されています。	○	-
12	Server unicast option	サーバは，クライアントがメッセージをサーバにユニキャストすることが許されるということをクライアントに知らせるために，クライアントにこのオプションを送ります。	-	-
13	Status Code	このオプションは，それが現れる DHCP メッセージまたはオプションに関連する状態表示の値を返します。	-	○
14	Rapid Commit	Rapid Commit オプションは，アドレス割り当てのための二つのメッセージ交換の使用を合図するのに使用されます。	○	○
15	User Class option	User Class オプションは，それが表すユーザまたはアプリケーションのタイプまたはカテゴリーを識別するために，クライアントによって使用されます。	○	-
16	Vendor Class Option	このオプションは，クライアントが動いているハードウェアを製造したベンダーを識別するために，クライアントによって使用されます。このオプションのデータ領域に含まれ 0 る情報は，ハードウェア構成の詳細を識別する一つ以上の不明瞭なフィールドに含まれます。	○	-
17	Vendor-specific Information option	このオプションは，vendor-specific 情報を交換するために，クライアントとサーバによって使用されます。	○	-
18	Interface-Id Option	リレーエージェントは，クライアントメッセージが受け取られたインタフェースを識別するために Interface-id オプションを送ることができます。リレーエージェントが Interface-id オプションを持つ Relay-reply メッセージを受け取った場合は，リレーエージェントはそのオプションによって識別されるインタフェースを通じて，クライアントにメッセージを転送します。	○※2	-
19	Reconfigure Message option	サーバは，クライアントが Renew メッセージか Information-request メッセージで応じるかどうかクライアントに示すために，Reconfigure Message に Reconfigure Message オプションを含めます。	-	-
20	Reconfigure Nonce option	サーバがセキュリティを Reconfigure Message に提供するために reconfigure nonce を使う場合に，サーバは各クライアントのために nonce 値を保持します。 サーバは，最初にクライアントに nonce 値を知らせて，それからクライアントに送るあらゆる Reconfigure Message に nonce 値を含めます。	-	-

Option Code	オプション名称	意味	値の設定側	
			クライアント（参考）	本装置（サーバ）
21	SIP Servers Domain Name List	そのクライアントが使用する SIP の outbound のプロキシサーバのドメインネーム。	○	◎
22	SIP Servers IPv6 Address List	このオプションは，クライアントに利用可能な SIP の outbound のプロキシサーバを示す IPv6 アドレスのリストを指定する。	○	◎
23	DNS Recursive Name Server	サーバが DNS サーバのアドレスをクライアントにリスト形式で渡す場合に指定するオプション。	○	◎
24	Domain Search List	クライアントはこのオプションを受け取ると，DNS によってホスト名の解決を行うときにこれに与えたドメインリストから検索します。このオプションはホスト名解決以外には使用すべきではありません。	○	◎
25	Identify Association for Prefix Delegation Option	Prefix Delegation アイデンティティ関連を配送するために使用するオプション。	○	◎
26	IA_PD Prefix Option	IPv6 アドレスプレフィックスが IA_ID との関連付けを指定します。	○	◎
31	Network Time Protocol (NTP) Servers	サーバがクライアントに対して NTP サーバのアドレスリストを通知するときに使用します。	○	◎

（凡例）

サーバ欄

◎：コンフィグレーションで設定する　○：自動的に設定する　△：クライアントから来た値を使用する　-：未サポート

クライアント欄

○：設定する　△：サーバから来た値を使用する　-：設定しない

注※１　DHCP Unique Identifier の略。

注※２　経由する DHCP リレーエージェントが設定する。

16.10.3　配布プレフィックスの経路情報

本装置は，クライアントのゲートウェイとして利用する場合に，配布したプレフィックスへの経路設定として次に示す 2 通りの方法を提供します。

- クライアントが経路情報の広告機能を保有しない場合
  本装置 DHCP サーバコンフィグレーションの配布プレフィックスへの経路自動設定機能を有効にすることで，配布先への経路が本装置に自動的に追加されます。
  また，このとき設定された経路のプリファレンス値は 250 固定となります。この機能で設定した経路以外のプリファレンス値については「表 16-23　各プロトコルで設定される経路のプリファレンス値」に示します。
- クライアントが経路情報の広告機能を保有する場合
  この場合，本装置～クライアント間で経路情報を交換し，経路を自動生成するため，本装置 DHCP サーバコンフィグレーションの配布プレフィックスへの経路自動設定機能は無効にします。

表 16-23　各プロトコルで設定される経路のプリファレンス値

経路	プリファレンス値	固定／可変
直結経路	0	固定
OSPFv3 の AS 内経路	10	可変
IS-IS の内部経路	15	可変
スタティック経路	60	可変
RIPng 経路	100	可変
集約経路	130	可変
OSPFv3 の AS 外経路	150	可変
IS-IS の外部経路	160	可変
BGP4+ 経路	170	可変
DHCPv6 サーバ自動設定	250	固定

16.10.4　DHCP サーバ機能使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

(1) 配布プレフィックスの使用状況の確認

本装置で配布できるプレフィックス総数は SB-7800S の場合 8,192 個，SB-5400S の場合最大 1,024 個です。配布していないプレフィックス個数は，運用コマンドの show ipv6 dhcp server statistics コマンドの実行結果「prefix pools」で確認できます。また，実際に配布されたプレフィックスは，show ipv6 dhcp binding コマンドで確認できます。

(2) DUID(DHCP Unique Identifier) について

本装置は DHCP で装置を区別するために使用するように規定される DUID を DHCP 機能が初めて導入されたときに生成します。生成した DUID は，プライマリ MC 中に静的に保存され，以後，運用コマンドから DUID の保存ファイルを削除するまで同じ値が使用されます。また，erase ipv6-dhcp server duid コマンドで DUID を削除した場合，show ipv6 dhcp server statistics コマンドで表示される Server DUID の値は，DUID を再生成するまで，削除する以前の値が表示されます。DUID の保存先や確認方法については，「運用ガイド　6.7.8 IPv6 DHCP サーバ機能を確認する」を参照してください。

(3) BCU 二重化時の系切替やサービス中の本装置再起動時の動作

本装置では，次に示す事象が発生した場合に制限事項があります。各状態の情報の保有性を次の表に示します。

表 16-24　各状態の情報の保有性

プレフィックスに関する保有情報	サーバ機能再起動		本装置再起動	BCU 二重化時の系切替
	コマンド投入	サーバ障害		
クライアントへの経路情報	○	△	×	△
クライアントへの配布情報	○	△	×	△

(凡例)　○：保証される　×：削除される
　△：保証される。ただし，一部 BCU 切り替え直前に配布したものについては保証されません。また，サーバ障害

時についても保証されません。

(4)　配布プレフィックスに対する経路自動設定機能使用時の注意

本装置では，クライアントに経路情報の広告機能がない場合など，特定条件下で経路情報の広告機能を使用せずに自動で経路情報を設定する機能がありますが，マルチパスや動的に経路が変更されるようなケースでは経路情報の広告機能を使用してください。

また，クライアントと本装置の間にほかの装置が存在する場合も，その装置に対する経路情報の広告は行われないため，経路情報の広告機能を使用してください。

(5)　IPv6 DHCP サーバと IPv6 PIM を同一インタフェースで使用する場合の注意事項

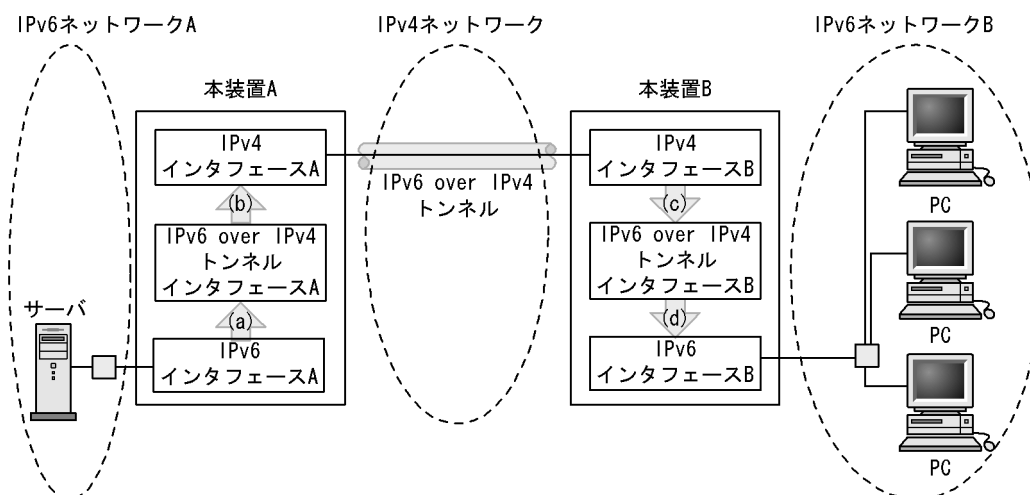
IPv6 PIM を有効にしたインタフェースで IPv6 DHCP サーバを使用する場合，IPv6 DHCP リレーからの DHCP 制御パケットは，全サーバ宛てマルチキャスト（FF05::1:3）ではなく，本装置のグローバルユニキャストアドレス宛てに送信してください。

16.11　トンネル

トンネルは，2 台以上の装置間に設定された入口／出口を通過するパケットを異なるプロトコルでカプセル化／非カプセル化することで，異なるプロトコルのネットワーク上に通信に使用できる回線を仮想的に設定できます。本装置では，RFC2473 に準拠した **Configured トンネル機能**と RFC3056 に準拠した **6to4 トンネル機能**をサポートしています。Configured トンネル機能には，IPv6 ネットワーク上で IPv4 パケットの通信を行う **IPv4 over IPv6 トンネル機能**と，IPv4 ネットワーク上で IPv6 パケットの通信を行う **IPv6 over IPv4 トンネル機能**があります。

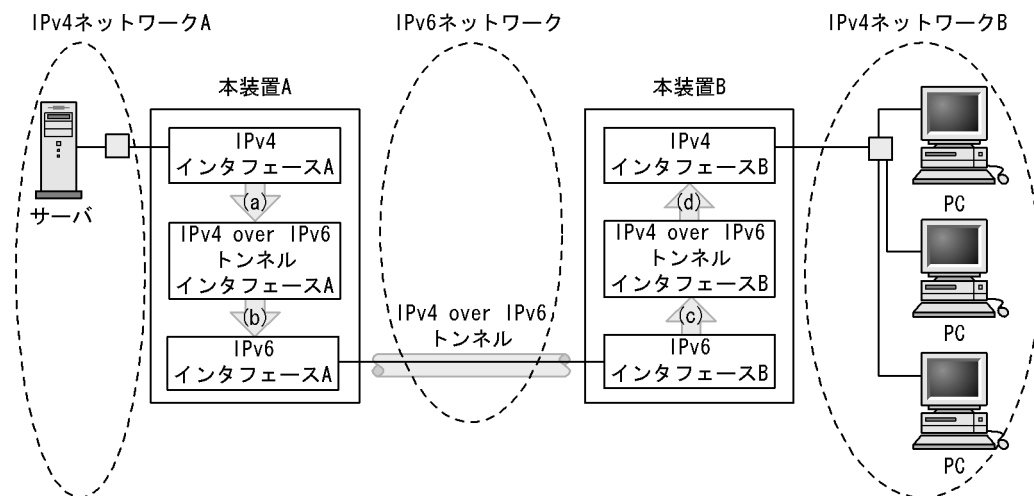
16.11.1　IPv6 over IPv4 トンネル

IPv6 over IPv4 トンネルは，IPv6 パケットを IPv4 によってカプセル化することで，IPv4 ネットワーク上に IPv6 パケットが通信可能な回線を仮想的に設定する機能です。トンネルの仮想インタフェースでは，IPv6 パケットを IPv4 でカプセル化し，また IPv4 パケットでカプセル化された IPv6 パケットを元に戻します。IPv6 over IPv4 トンネルのパケット状態を次の図に示します。

図 16-27　IPv6 over IPv4 トンネルのパケット状態

(a)　IPv6インタフェースAで受信したIPv6パケットの宛先アドレスと経路情報より送信インタフェースをIPv6 over IPv4トンネルインタフェースAと判断する。
(b)　IPv6 over IPv4トンネルインタフェースAでIPv6パケットをIPv4でカプセル化し，トンネル情報で指定したIPv4インタフェースAより本装置B宛てのIPv4パケットとして送信する。
(c)　IPv4インタフェースBでは，受信したIPv4パケットのヘッダと送信元アドレスをチェックし，カプセル化されたパケットであれば指定されたIPv6 over IPv4トンネルインタフェースBへ送る。
(d)　IPv6 over IPv4トンネルインタフェースBで受信したIPv4パケットのカプセル化を解除し，元のパケットの宛先アドレスと経路情報より送信インタフェースをIPv6インタフェースBと判断し，IPv6パケットを送信する。

16.11.2　IPv4 over IPv6 トンネル

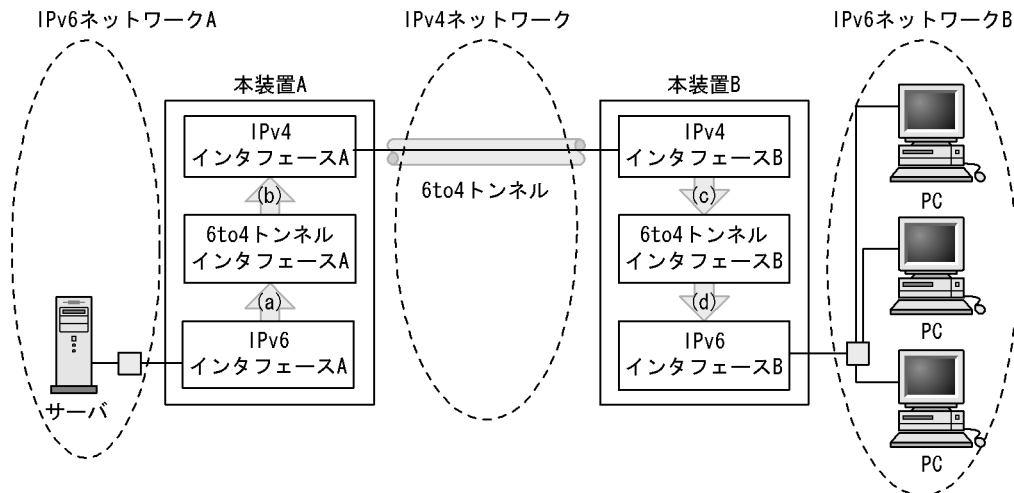
IPv4 over IPv6 トンネルは，IPv4 パケットを IPv6 によってカプセル化することで IPv6 ネットワーク上に IPv4 パケットが通信できる回線を仮想的に設定する機能です。トンネルの仮想インタフェースでは，IPv4 パケットを IPv6 でカプセル化し，また IPv6 パケットでカプセル化された IPv4 パケットを元に戻します。IPv4 over IPv6 トンネルのパケット状態を次の図に示します。

図 16-28　IPv4 over IPv6 トンネルのパケット状態

(a) IPv4インタフェースAで受信したIPv4パケットの宛先アドレスと経路情報より，送信インタフェースをIPv4 over IPv6トンネルインタフェースAと判断する。
(b) IPv4 over IPv6トンネルインタフェースAでIPv4パケットをIPv6でカプセル化し，トンネル情報で指定したIPv6インタフェースAより本装置B宛てのIPv6パケットとして送信する。
(c) IPv6インタフェースBでは，受信したIPv6パケットのヘッダおよび送信元アドレスをチェックし，カプセル化されたパケットであれば指定されたIPv4 over IPv6トンネルインタフェースBへ送る。
(d) IPv4 over IPv6トンネルインタフェースBで受信したIPv6パケットのカプセル化を解除し，元のIPv4パケットの宛先アドレスと経路情報より送信インタフェースをIPv4インタフェースBと判断し，パケットを送信する。

16.11.3　6to4 トンネル

6to4 トンネルは，使用する IPv4 ネットワークに定義されている IPv4 アドレスから，固有の IPv6 アドレス (6to4 アドレス) を決定するため，新しく IPv6 アドレスを割り当てる必要がありません。この機能の特徴は，IPv4 ネットワークを一つのユニキャストポイント - ポイント型リンク層として扱うことです。6to4 トンネルは，専用に割り当てられたプレフィックス 2002::/16 と IPv4 グローバルユニキャストアドレスから専用の IPv6 アドレスである 6to4 アドレスを持ちます。なお，6to4 トンネルと Configured トンネルは混在できます。

トンネルの仮想インタフェースでは，6to4 アドレス内の IPv4 アドレスを基に IPv6 パケットを IPv4 でカプセル化し，また IPv4 パケットでカプセル化された IPv6 パケットを元に戻します。6to4 トンネルのパケット状態を次の図に示します。

図 16-29　6to4 トンネルのパケット状態

(a)　IPv6インタフェースAで受信したIPv6パケットの宛先アドレスと経路情報より送出インタフェースを6to4トンネルインタフェースAと判断する。
(b)　6to4トンネルインタフェースAでIPv6パケットをIPv4でカプセル化し，6to4アドレスで指定したIPv4インタフェースAより装置B宛てのIPv6パケットとして送出する。
(c)　IPv4インタフェースBでは，受信したIPv4パケットのヘッダとカプセル化されたIPv6パケットのアドレスをチェックし，6to4トンネルでカプセル化されたパケットであれば，指定された6to4トンネルインタフェースBへ送る。
(d)　6to4トンネルインタフェースBで受信したIPv4パケットのカプセル化を解除し，元のIPv6パケットの宛先アドレスと経路情報より送出インタフェースをIPv6インタフェースBと判断し，パケットを送出する。

16.11.4　トンネル機能使用時の注意事項

トンネル機能を使用するときの注意事項を次に示します。

（1） トンネル機能を使用できない構成

トンネル機能を使用する場合，いくつかの禁止構成があります。装置に設定するトンネルの数が多くなると禁止構成の判別が難しくなりますが，次の点に着目して判断します。

1. **トンネル設定で，別のトンネルの仮想インタフェースをパケット送受信インタフェースに指定しない**
   トンネルの仮想インタフェースでカプセル化されたパケットの送受信インタフェースを，別のトンネルの仮想インタフェースに指定した場合パケットが多重にカプセル化されることになり，正常に通信ができません。
2. **同一装置内で多重にカプセル化を行わない**
   同一装置内で，トンネルの仮想インタフェースでカプセル化されたパケットが再度別のトンネル仮想インタフェースでカプセル化が行われる場合，パケットが多重にカプセル化されることになり，正常に通信ができません。
3. **トンネルを設定した装置間にアドレス変換機能 (NAT 機能など) を使用した装置を置かない**
   アドレス変換機能でヘッダ情報を書き換えると，カプセル化されたパケットのヘッダの値が異常となる場合があります。
4. **同一プロトコルによるトンネル設定**
   トンネルで設定された仮想インタフェースに設定されたプロトコルと，パケット送受信インタフェースに指定されたプロトコルが同一プロトコルとなる IPv4 over IPv4 トンネル，または IPv6 over IPv6 トンネルにはならないようにしてください。
5. **トンネルインタフェースでのマルチキャストパケット中継**

トンネルインタフェースでのマルチキャストパケット中継はサポートしていません。IPv4 over IPv6 トンネルを使用しているネットワーク構成では，該当するトンネルインタフェースで IPv4 マルチキャストパケットへ中継することはできません。また，IPv6 over IPv4 トンネルおよび 6to4 トンネルでは，該当するトンネルインタフェースで IPv6 マルチキャストパケットへ中継することはできません。

6. **トンネルインタフェースの扱い**
   トンネルインタフェースはコンフィグレーションで指定した相手アドレスに対して到達可能かどうかに関係なく，常に Up 状態になります。そのため物理インタフェースでの疎通ができなくなった場合に，該当するトンネルインタフェースを使用している RIPng，OSPFv3，BGP4+ などによる経路情報が別のインタフェースを使用するまでにかかる時間は，通常の物理インタフェースを使用した場合の経路変更と比較して長くなる場合があります。
   なお，6to4 トンネルインタフェースは，対応する物理インタフェースの状態に依存します。このため，対応の物理インタフェースが Up 状態であれば Up，Down 状態であれば Down となります。
7. **6to4 トンネル経由の経路交換**
   6to4 トンネルのインタフェースには 6to4 アドレスしか定義できません。また，リンクローカルアドレスも自動設定されません。したがって，リンクローカルアドレスを使った RIPng，OSPFv3 によって経路交換を行うことはできません。また，BGP4+ による経路交換もサポートしていません。
8. **トンネルインタフェースでのフラグメントパケットの扱い**
   トンネルパス上の経路が安定していない，マルチパス構成上の経路を通るなどの場合，同一インタフェースからすべてのフラグメントパケットを受信できるとは限りません。この場合該当パケットは破棄されますので，フラグメントの発生を避けるようにシステム構築してください。
9. **VRRP 使用時の注意点**
   - トンネルインタフェースは VRRP のクリティカルインタフェースに使用できません。
   - VRRP で設定した仮想インタフェースの IPv4 アドレスは 6to4 トンネルに使用できません。
10. **6to4 サポート対象外インタフェースについて**
    次に示すインタフェース上で 6to4 トンネルは動作しません。このため，これらのインタフェースに定義している (動的割り当ての場合は割り当てられた IPv4 アドレス) を，6to4 プレフィックスに使用しないでください。
    - IPv4 アドレスが動的割り当てで決定するインタフェース (DHCP)
    - rmEthernet
    - unnumbered インタフェース

（2） 6to4 トンネル使用時のセキュリティについて

6to4 アドレスはインターネットを仮想的に一つのデータリンクとして使用します。そのため，基本的にインターネットと接続しているすべての端末と接続することになります。6to4 トンネル経由での通信相手が特定できる場合は，6to4 トンネルを構成する IPv4 アドレスでフィルタリングを行うなどの対策をしてください。

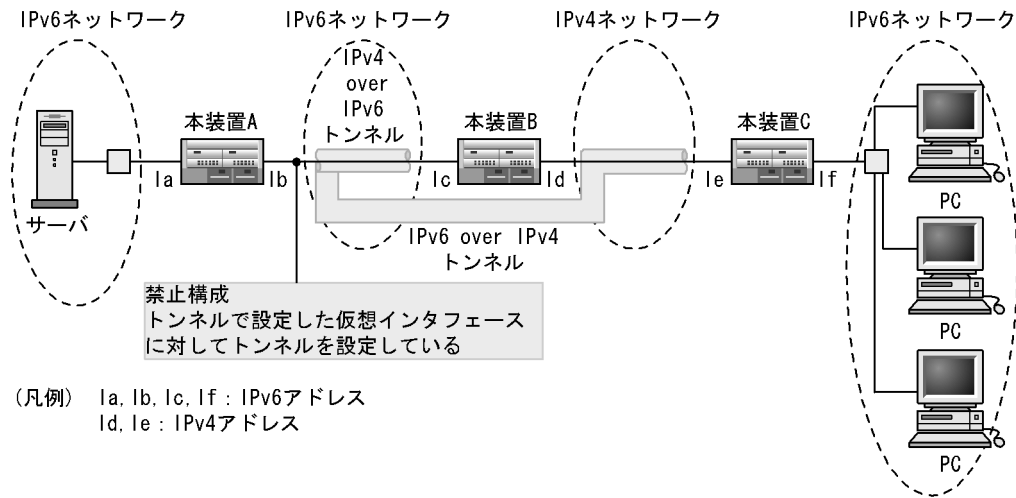
（3） 多重トンネル

あるトンネルの仮想インタフェースを，別のトンネルの仮想インタフェースでカプセル化されたパケットの送受信インタフェースに指定する多重トンネルは使用できません。

（a） 構成例 1

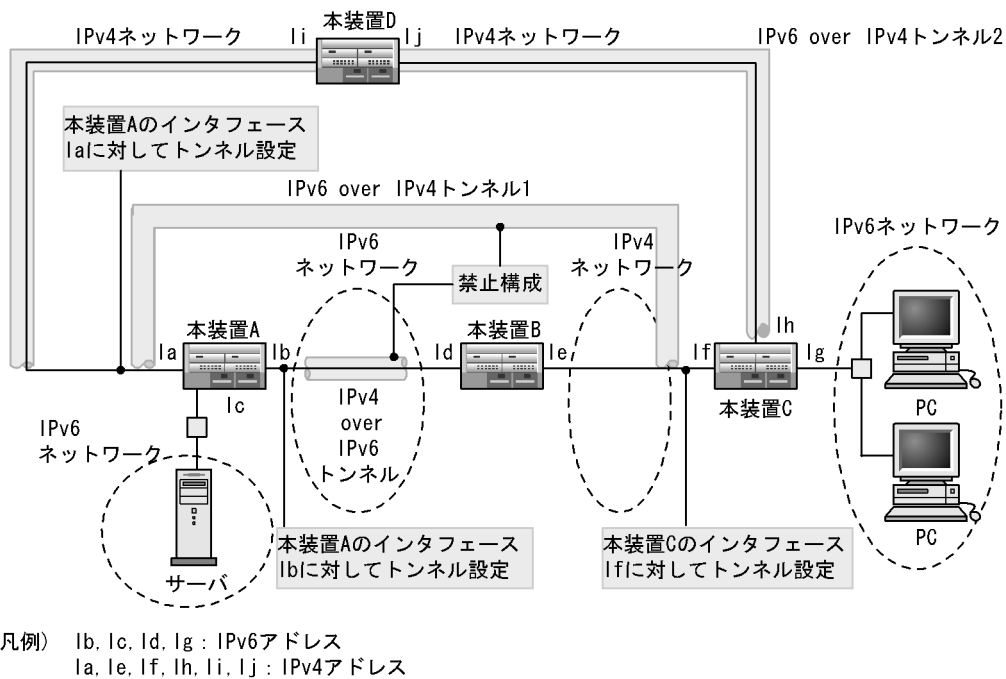
トンネルの仮想インタフェースに設定されているアドレスは，別のトンネルの仮想インタフェース設定時には指定しないでください。多重トンネル禁止構成例を次の図に示します。

図 16-30　多重トンネル禁止構成例 1

注意点

本装置 A のインタフェース Ib をパケット送受信インタフェースとして指定した，本装置 A と本装置 B 間の IPv4 over IPv6 トンネル仮想インタフェースを設定します。その仮想インタフェースを，本装置 A と本装置 C 間の IPv6 over IPv4 トンネルのパケット送受信インタフェースとして指定する設定を行います。このような構成では，本装置 A から本装置 C へ中継されるパケットは本装置 A 内で二つのトンネルインタフェースで多重にカプセル化が行われる多重トンネル構成になります。

(b)　構成例 2

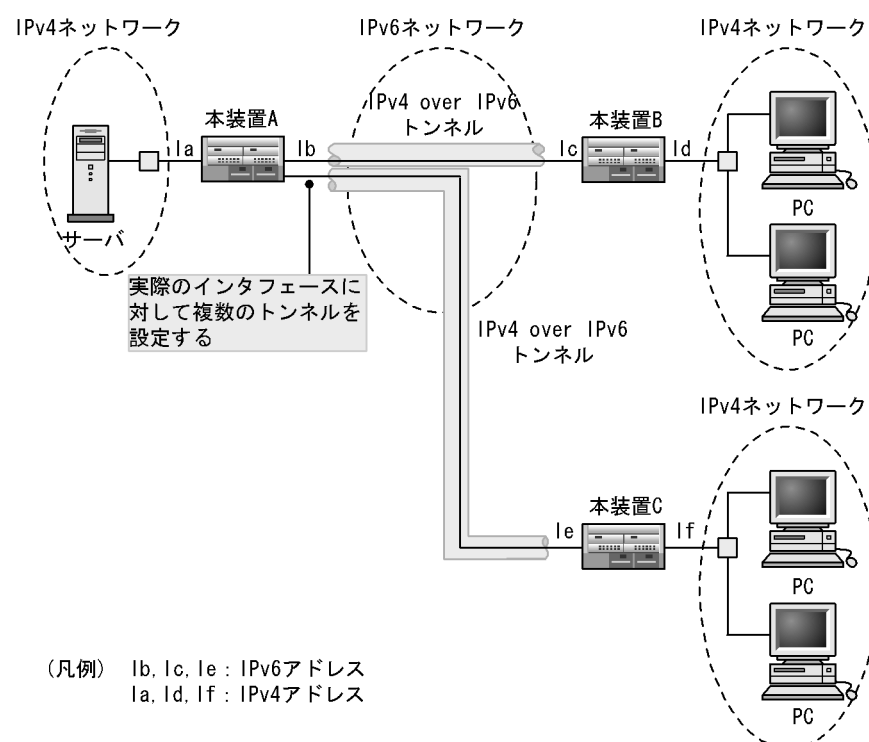
トンネルを設定した装置間の到達経路が複数ある構成で，ある一方の経路が同一装置内を始点とするトンネルを通過するような構成の場合，経路情報の変化によって多重トンネル構成になる場合があるので注意してください。多重トンネル禁止構成例を次の図に示します。

図 16-31　多重トンネル禁止構成例 2

注意点

本装置 A と本装置 C 間に設定した IPv6 over IPv4 トンネルは経路情報によってトンネル 1 またはトンネル 2 のどちらかの経路を通過します。トンネル 1 の状態となったとき，本装置 C 向けトンネルの経路は本装置 A と本装置 B 間に設定された IPv4 over IPv6 トンネルを通過する経路となってしまうため，パケットは本装置 A 内で二つのトンネルインタフェースで多重にカプセル化が行われる多重トンネル構成になります。

(c) 構成例 3

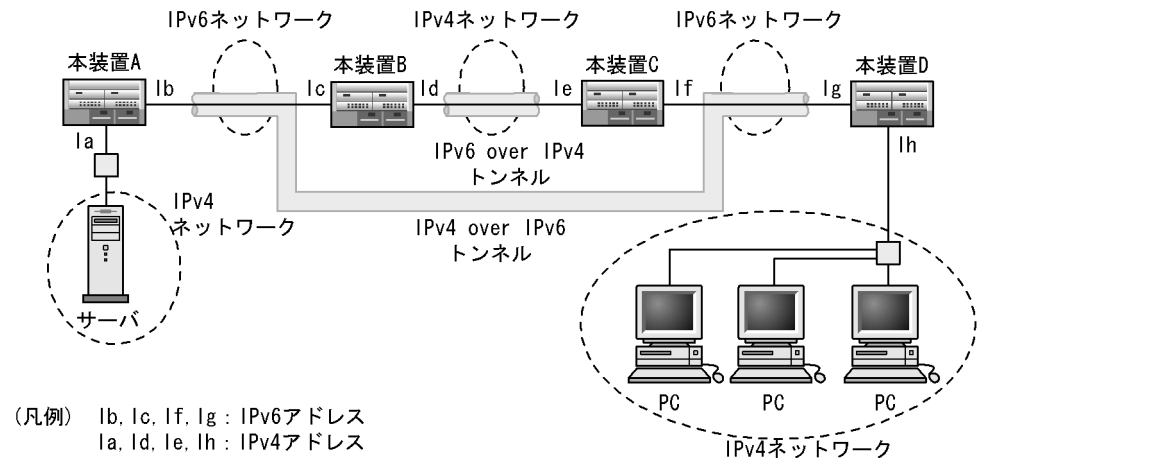
トンネルの仮想インタフェース以外のインタフェースをカプセル化されたパケットの送受信インタフェースに指定する場合は，同一インタフェースに複数指定しても多重トンネル構成にはなりません。多重トンネルにならない構成例を次の図に示します。

図 16-32 多重トンネルにならない構成例 1

注意点

本装置 A と本装置 B，本装置 C それぞれの間に設定された IPv4 over IPv6 トンネルを中継されるパケットは，本装置 A 内でカプセル化されるのは 1 度だけです。また，本装置 A 内で，各装置への到達経路に別のトンネルが設定されていないため，この構成は多重トンネル構成にはなりません。

(d) 構成例 4

トンネルを設定した装置間の，中継経路上の別の装置間でトンネルが設定されている場合は多重トンネル構成にはなりません。多重トンネルにならない構成例を次の図に示します。

図 16-33　多重トンネルにならない構成例２

注意点

本装置 A と本装置 D 間に IPv4 over IPv6 トンネルの経路途中に別のトンネルが設定されていますが，各装置内でカプセル化を行うのは１度だけのため，多重トンネル構成にはなりません。本装置 B と本装置 C 間の IPv4 over IPv6 トンネルに本装置 A と本装置 D 間の IPv4 over IPv6 トンネルでカプセル化されたパケットが中継されますが，本装置 B と本装置 C ではカプセル化されたパケットとして意識しないで通常の IPv6 パケットとして IPv4 でカプセル化を行います。

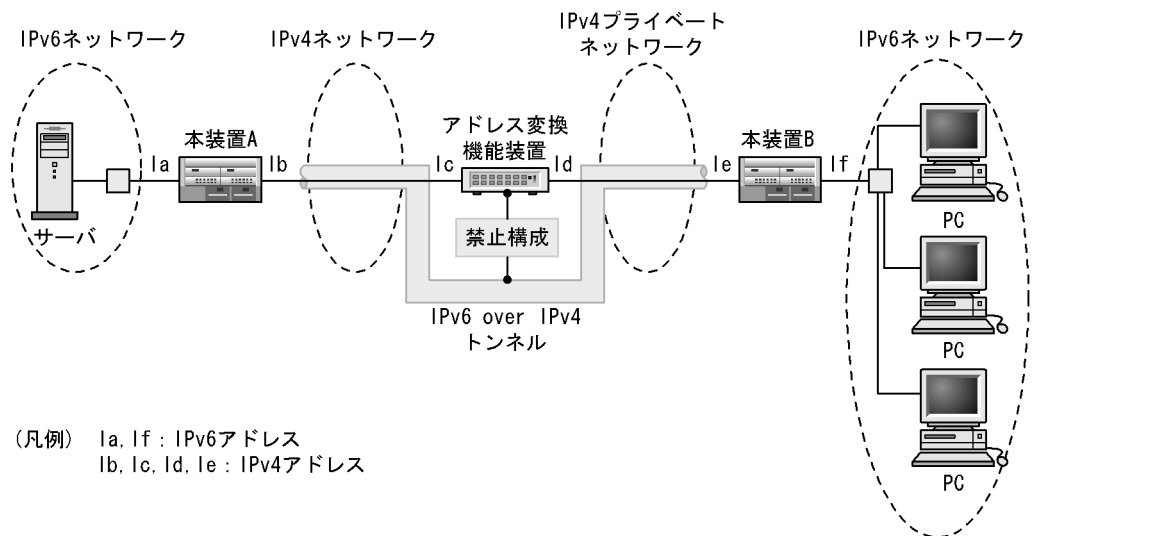
(4) アドレス変換機能を使用した装置をはさんだ構成

アドレス変換を行ったアドレスをトンネルの接続先には指定できません。

(a) 構成例 1

トンネルを設定している装置間にアドレス機能変換を持つ装置を設置し，アドレス変換を行ったアドレスをトンネルの接続先として指定しないでください。

アドレス変換機能装置によってパケット内のヘッダ情報が書き換えられることでトンネルを設定した装置間で通信ができなくなります。トンネル間にアドレス変換機能装置のある禁止構成例を次の図に示します。

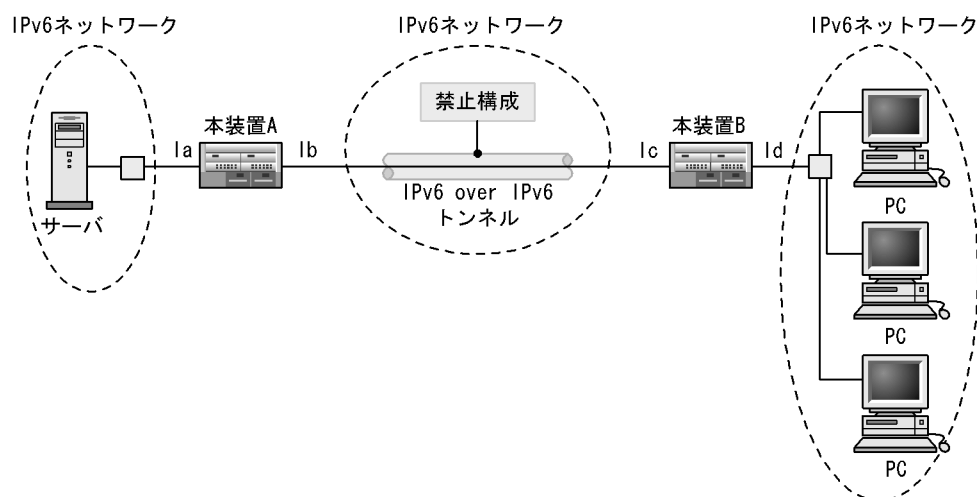
図 16-34　トンネル間にアドレス変換機能装置のある禁止構成例

注意点

本装置 A のトンネル設定で，カプセル化したパケットの宛先アドレスを，アドレス変換機能を使用したプライベートネットワーク内のアドレスとした場合，トンネルの仮想インタフェースでカプセル化されたパケットのヘッダ情報がアドレス変換機能装置によって書き換えられます。このため，本装置 A と本装置 B 間でのトンネルによる中継ができなくなります。

(5) 同一プロトコルによるトンネル設定

(a) 構成例 6

トンネルの仮想インタフェースでカプセル化したパケットのプロトコル種別と，パケット送受信インタフェースに指定されたインタフェースに設定されているプロトコルが同一の場合，パケットを同一のプロトコルでカプセル化することになって，正常に中継できない恐れがあります。IPv6 の場合の同一プロトコルによるトンネル禁止構成例を次の図に示します。

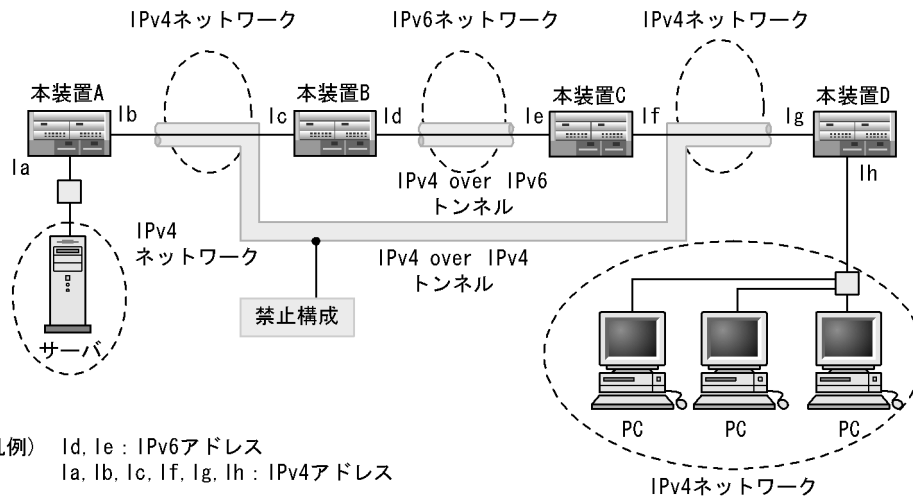
図 16-35 同一プロトコルによるトンネル禁止構成例 (IPv6 over IPv6 トンネル)

注意点

本装置 A の IPv6 インタフェース Ib と本装置 B の IPv6 インタフェース Ic をトンネルの仮想インタフェースでカプセル化されたパケットの送受信インタフェースとして指定します。次に，トンネル仮想インタフェースのアドレス設定で IPv6 アドレスを設定すると，パケット送受信インタフェースと同じプロトコルを指定した IPv6 over IPv6 トンネル構成となるため，パケットが正常に中継されません。

(b) 構成例 7

IPv4 の場合の同一プロトコルによるトンネル禁止構成例を次の図に示します。

図 16-36 同一プロトコルによるトンネル禁止構成例 (IPv4 over IPv4 トンネル)

（凡例） Id, Ie : IPv6アドレス
Ia, Ib, Ic, If, Ig, Ih : IPv4アドレス

注意点

本装置 A の IPv4 インタフェース Ib と本装置 D の IPv4 インタフェース Ig をトンネルの仮想インタフェースでカプセル化されたパケットの送受信インタフェースとして指定します。次に，トンネル仮想インタフェースのアドレス設定で IPv4 アドレスを設定すると，パケット送受信インタフェースと同じプロトコルを指定した IPv4 over IPv4 トンネル構成となるため，パケットが正常に中継されません。

16.12　RA

RA(Router Advertisement) は，ルータが端末群に IPv6 アドレス生成に必要な情報やデフォルトルートを配布する機能であり，DHCP(Dynamic Host Configuration Protocol) でのアドレス設定やデフォルトルート配布の機能に相当します。

● DHCP 方式

サーバで管理される複数のアドレスのどれかを割り当ててもらう方式です。

DHCP ではルータとは別に DHCP サーバを設置する必要があります。また，アドレスを要求する端末が DHCP サーバに対してアドレスを要求し，DHCP サーバからアドレスそのものを配布します。

● RA 方式

ルータから通知されるプレフィックスと端末自身が生成したアドレスの後半を組み合わせて，インタフェースのアドレスを決定する方式です。

RA ではルータがアドレスのプレフィックス部だけを一定間隔で配布し，各端末が固有のインタフェース ID 部と受信した RA 内のプレフィックス情報から端末でアドレスを生成します。こうした特徴によって，RA はサーバレスで端末数に依存しない簡便な Plug & Play を実現します。なお，RA によるアドレス自動設定はルータ以外の端末だけで設定でき，ルータは RA を受信してもアドレスを自動設定しません。

DHCP 方式のアドレス設定を「図 16-37　DHCP 方式のアドレス設定」に，RA 方式のアドレス設定を「図 16-38　RA 方式のアドレス設定」に示します。

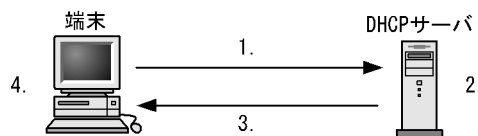
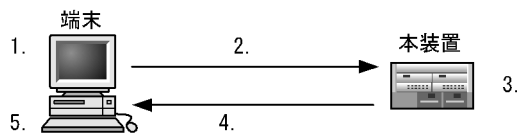
図 16-37　DHCP 方式のアドレス設定

1. 使用できるアドレス1個を要求する。
2. 設定されているアドレスリストより端末に指定するアドレスを決定する。
3. 使用するアドレスを通知する。
4. 通知されたアドレスを設定する。

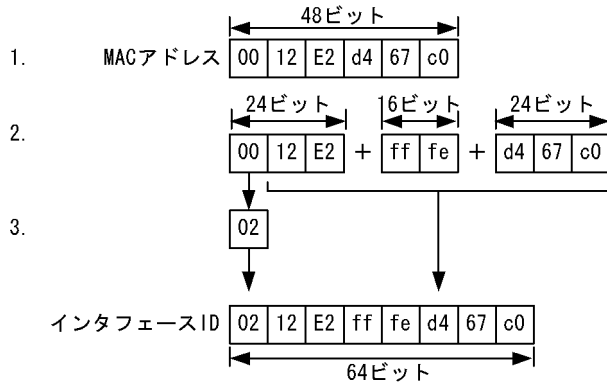
図 16-38　RA 方式のアドレス設定

1. インタフェースIDを生成する。
2. プレフィックスを要求する。
3. RAで配布するプレフィックスを設定する。
4. プレフィックスを通知する。
5. 通知されたプレフィックスとインタフェースIDを組み合わせてアドレスを生成し，設定する。

16.12.1　RA によるアドレス情報配布

RA によるアドレス配布には，ルータからの定期的な配布と，端末からのリクエストに対するルータの応答の 2 種類があります。両者は配布の契機が異なるだけで，どちらの場合も，ルータからのアドレス配布

は ICMPv6 パケット Type 134 で規定された RA によって行われます。また，端末からのリクエストは ICMPv6 パケット Type133 の RS(Router Solicitation) によって行われます。

RA を受信した端末は，与えられたプレフィックスと各端末で固有である 64 ビットのインタフェース ID(通常は 48 ビットの MAC アドレスを基に生成) を組み合わせたグローバルアドレスを生成し，RA を受信したインタフェースに設定します。同時に RA 送信元アドレス (=RA を送信したルータのインタフェースリンクローカルアドレス) を端末のデフォルトゲートウェイとして設定します。MAC アドレスからのインタフェース ID 生成を次の図に示します。

図 16-39　MAC アドレスからのインタフェース ID 生成

1.MACアドレスを24ビットで二つに分割する。
2.中間に固定値"ff fe"を挿入する。
3.最初の8ビットの下位2ビット目の値を反転する。

ルータから端末に伝えられるプレフィックスは，通常は RA を広告するインタフェースに定義されたアドレスプレフィックスのうち，リンクローカルを除いたものです。ただし，それに加えてそのほかのプレフィックスを広告することもできます。また，ルータからの RA 送出時間間隔の最大値，最小値をインタフェース単位で設定できます。RA で配布される情報を次の表に示します。

表 16-25　RA で配布される情報

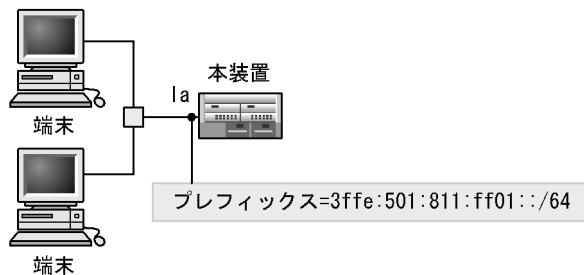
配布情報	説明	設定できる範囲	省略時の初期値
アドレス自動管理設定フラグ (managed-flag)	RA 以外の方法 (DHCPv6 など) による IPv6 アドレス設定を，RA 受信を契機に端末で自動的に行わせることを指定するフラグ。 このフラグの値に関係なく，RA によるアドレス設定は必ず行われます。通常は OFF にしてください。	ON/OFF	OFF
アドレス以外情報設定フラグ (other-flag)	RA 以外の方法 (DHCPv6 など) による IPv6 アドレス以外の情報 (DNS サーバなど) を，RA 受信を契機に端末で自動的に行わせることを指定するフラグ。通常は OFF にしてください。	ON/OFF	OFF
リンク MTU (link-mtu)	端末が実際の通信に使 MTU 値を指定します。通常使用される MTU 値は RA を受信したインタフェースの MTU 値ですが，インタフェースの MTU いっぱいのパケットを端末に使わせたくない場合に，このパラメータを MTU 値よりも小さい値に設定します。インタフェースの MTU よりも大きい値を通知することはできません。	1280 〜インタフェースの MTU	配布しない

配布情報	説明	設定できる範囲	省略時の初期値
可到達時間 (reachable-time)	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，その確認結果の有効期間を端末に指定します。未指定または 0 を指定した場合は端末ごとに定められたデフォルト値が到達性確認結果の有効期間になります。	0 ～ 3600000（秒）	配布しない
再送時間 (retrans-timer)	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，そのとき送信する ICMPv6 パケットの送信間隔を端末に指定します。未指定または 0 を指定した場合は端末ごとに決められたデフォルト値が再送間隔として使用されます。	0 ～ 4294967295（秒）	配布しない
端末ホップリミット (curhoplimit)	端末がパケットを送信するときに，何ホップ先まで中継できるかを示す IPv6 ヘッダ内のホップリミット領域に設定する値を指定します。	0 ～ 255	64
ルータ生存時間 (lifetime)	端末が RA によって確定したデフォルトルータの有効期間。0 を指定すると，端末は，受信した RA の送信元アドレスをデフォルトゲートウェイとみなしません。	0 ～ 9000（秒）	RA 送出間隔の最大値の 3 倍
リンク層オプション (advlinkopt)	RA 送信元の IPv6 アドレスに対応するリンク層アドレス。本装置の場合は，RA 広告インタフェースがイーサネットおよびギガビット・イーサネットの場合だけ，そのポートの MAC アドレスが入ります。このオプションを OFF にすると，各端末でデフォルトゲートウェイのリンク層アドレス解決が行われます。そのためリンク層アドレスによる負荷分散を行えます。本装置ではオプションを OFF に指定していますが，ロードバランス機能はサポートしていません。	ON/OFF	ON
ルータ優先度 (router-preference)	端末が複数ルータより RA を受信した場合に，どの RA の情報を優先して使用するか指定します。	high，medium，low	medium
プレフィックス	RA で広告するプレフィックス。指定していないときは，広告するインタフェースについているリンクローカルではないプレフィックスを広告します。それ以外に，さらにプレフィックスを広告したい場合や，インタフェースについているプレフィックスに対して有効期間を設定する場合に使用します。	グローバル，サイトローカルプレフィックス	インタフェースの非リンクローカルプレフィックス
自律設定有効フラグ (autonomous-flag)	このオプションが OFF のプレフィックスは端末に付与されません。RA の試験運用以外のときは常時 ON にしてください。	ON/OFF	ON
オンリンクフラグ (onlink-flag)	このオプションが OFF のプレフィックスについては，端末での redirect メッセージの送信が抑制されます。RA の試験運用以外の時は常時 ON にしてください。	ON/OFF	ON
推奨有効期間 (preferred-lifetime)	RA によって通知されたプレフィックスを，端末が通信時のソースアドレスに使用することを許可する時間。推奨する有効期間を過ぎても RA を受信しないと，該当するプレフィックス以外のアドレスを通信のソースアドレスとして使用することを試行します。ただし，ほかに適切なプレフィックスを持たない場合は，端末は推奨する有効期間を過ぎたプレフィックスを通信に使用します。	RA 送出間隔の最大値～ 4294967296(秒）	604800

配布情報	説明	設定できる範囲	省略時の初期値
最終有効期間 (valid-lifetime)	RA によって通知されたプレフィックスが消滅するまでの時間。最終有効期間を過ぎても RA を受信しないと，端末は該当するプレフィックスのアドレスを削除します。	RA 送出間隔の最大値～4294967296(秒)	2592000

16.12.2 RA 情報変更時の例

RA で端末にプレフィックスを配布している構成では，プレフィックスの値を変更すると，急なアドレス変更によって疎通できなくなることがあります。それを防ぐために標準設定では古いプレフィックスが 604800 秒 (7 日間) 残るようになっています。古いプレフィックスを削除するには，変更対象のプレフィックスと同時に新しいプレフィックスを広告し，有効時間を徐々に変更することで古いプレフィックスを削除してください。RA の使用例を次の図に示します。

図 16-40　RA の使用例

1. イーサネットのインタフェース Ia から RA をネットワークに広告する定義を行います。
   - Ia のプレフィックス = 3ffe:501:811:ff01::/64
2. Ia のプレフィックスを 3ffe:501:811:ff01::/64 から 3ffe:501:811:ff22::/64 に変更する定義を行います。
   - Ia で新しく広告するプレフィックス 3ffe:501:811:ff22::/64 の広告間隔を短く設定し，広告を開始します。
   - Ia で利用を停止するプレフィックス 3ffe:501:811:ff01::/64 の推奨有効期間 , 最終有効期間を短く設定して広告を行います。
   - Ia での 3ffe:501:811:ff22::/64 の広告間隔をデフォルト値に戻します。
   - 広告を終了するプレフィックス 3ffe:501:811:ff01::/64 の広告を停止します。

16.12.3 RA の送信間隔

RA を広告する相手端末数に応じて，RA の送信間隔が制限されます。詳細は，「コンフィグレーションコマンドレファレンス Vol.1　11. RA 情報」のコンフィグレーションコマンド ra を参照してください。

16.13　IPv6 使用時の注意事項

（1） IPv6 中継回線の MTU 長の変更

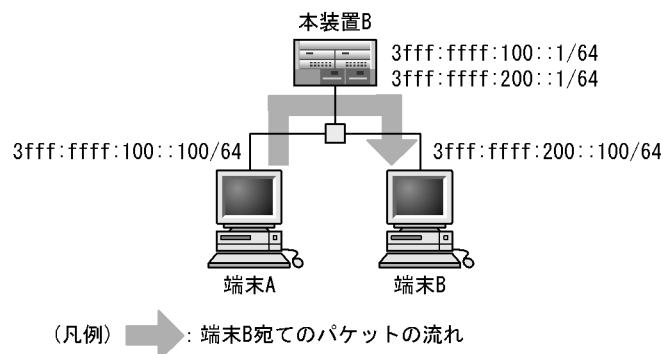
IPv6 の最小パケット長は 1280 バイト以上と規定されています (RFC2460)。このため，ATM 回線の VC など MTU 長を変更できるインタフェースで MTU 長を 1280 バイト未満に設定すると，IPv6 通信ができません。IPv6 通信を行うインタフェースの MTU 長は 1280 バイト以上で使用してください。

（2） 同一リンクでのハードウェア中継機能

同一リンク上の本装置および端末間の IPv6 通信について，本装置が IPv6 ハードウェア中継を行う場合，次に示す注意事項があります。

（a） 同一リンク上の端末間の通信

次に示す図のような構成で，同一リンク上の IPv6 端末間で行う通信のプレフィックスが一致していないために本装置に中継させる設定をしている場合，ハードウェアによる高速中継にはなりません。このため，性能が低下する場合があります。同一リンク上の IPv6 端末上の通信では各端末の IPv6 アドレスのプレフィックスを一致させ，端末同士が直接通信する設定にしてください。

図 16-41　同一リンク上の IPv6 端末間の通信に本装置を使用する構成

（b） ICMPv6 リダイレクトメッセージ送信

ICMPv6 リダイレクトメッセージが送信されるのは，ネクストホップアドレスが同一リンク上のルータのリンクローカルアドレスの場合だけです。経路のネクストホップアドレスをグローバルアドレスで設定している場合は，ICMPv6 リダイレクトメッセージが送信されないので注意してください。

（3） ping ipv6 および traceroute ipv6 コマンドの宛先 IPv6 アドレス

本装置では，インタフェース立ち上がり時に RFC2462 で規定されている重複アドレス検出を実行します。これによって他装置との重複が確認された IPv6 アドレスに対して ping ipv6 および traceroute ipv6 コマンドを実行した場合，宛先として指定した IPv6 アドレスではなく，本装置の別のインタフェースの IPv6 アドレスから返答が返ることがあるので注意してください。

また，インタフェース立ち上がり直後の数秒間は，重複アドレス検出が完了していないため，同様に別の IPv6 アドレスから返答が返ることがありますが，重複アドレス検出が完了次第通常の動作に戻るので問題ありません。

（4） 送信元アドレスと宛先アドレスのスコープが異なるパケットの扱い

本装置では，送信元アドレスがリンクローカルアドレスで，宛先アドレスがリンクローカルアドレス以外

のパケットは不正なパケットとして廃棄します。しかし，送信元アドレスに対して ICMPv6 Destination Unreachable (beyond scope of source address) メッセージを返しません。

(5) IPv6 拡張オプション付きパケットのレイヤ 3 中継

1. 中継点オプション付きパケットをレイヤ 3 中継する場合，ソフトウェア中継になります。
2. 受信側の QoS 制御機能を使用している場合，経路制御オプションまたは終点オプションを付加している TCP パケットのレイヤ 3 中継は，ソフトウェア中継になります。

(6) インタフェースへのグローバルアドレスの設定

インタフェースにグローバルアドレスを設定する際は，同一リンク上のインタフェースのプレフィックスおよびプレフィックス数が，全装置で同じになるようにしてください。この条件を満たさない場合，本装置に存在しないインタフェースのプレフィックスに対して通信ができません。

17 RIPng/OSPFv3

この章では，主にイントラネットに適用されるルーティングプロトコルである RIPng，OSPFv3 について説明します。

17.1 IPv6 ルーティング

IPv6 ルーティングプロトコルの概要について説明します。

17.1.1 スタティックルーティングとダイナミックルーティング

パケットを中継するためにはルーティングテーブルを作成する必要があります。本装置のルーティングテーブルの作成方法は，大きくスタティックルーティングとダイナミックルーティングに分類できます。

- スタティックルーティング
  ユーザがコンフィグレーションによって経路情報を設定する方法です。
- ダイナミックルーティング
  ネットワーク内のほかのルータと経路情報を交換して中継経路を決定する方法です。本装置は RIPng, OSPFv3(バージョン 3)，BGP4+(バージョン 4+)，IS-IS をサポートしています。

17.1.2 経路情報

本装置が取り扱う経路情報，つまりルーティング対象とするアドレスの種類を次に示します。本装置はサイトローカルアドレスをグローバルアドレスと同様に扱います。

- デフォルト経路
  すべてのネットワーク宛ての経路。(宛先プレフィックス ::/0)
- グローバルネットワーク経路
  特定のネットワーク宛てのグローバル経路，および複数のネットワーク宛てのグローバル経路を集約したもの。
- グローバルホスト経路
  特定のホスト宛てのグローバル経路。(プレフィックス長が 128 ビットのグローバル経路)

17.1.3 ルーティングプロトコルごとの適用範囲

本装置のサポートするルーティングプロトコルについて取り扱う経路情報および機能の概要を次の表に示します。

表 17-1 ルーティングプロトコルごとの適用範囲

経路情報		スタティック	ダイナミック	
			RIPng	OSPFv3
経路情報	デフォルト経路	○	○	○
	グローバルネットワーク経路	○	○	○
	グローバルホスト経路	○	○	○
	マルチパス	○	×	○
経路選択		-	メトリック（経由するルータ数）	コスト（経由するルータ数および回線速度）
ルーティングループ抑止		-	スプリットホライズン	○
認証機能		-	×	×

（凡例） ○：取り扱う ×：取り扱わない -：コンフィグレーションによるので該当しない

17.2　ネットワーク設計の考え方

17.2.1　アドレス設計

IPv6 アドレス割り当て時には次のような考え方に従うと，注意しなければならない事項の多くを回避でき，比較的簡単にネットワーク設計をすることができます。

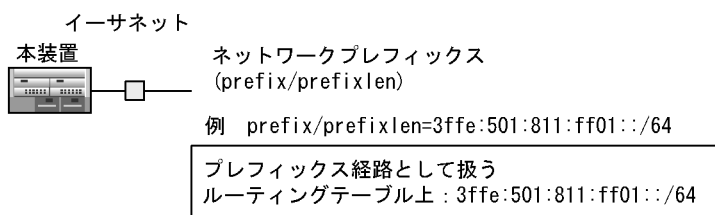
- NLA や SLA を，ネットワークトポロジの階層構造に従って分割します。
- ポイント - ポイント型の回線は極力リンクローカルアドレスだけを割り当てます。

17.2.2　直結経路の取り扱い

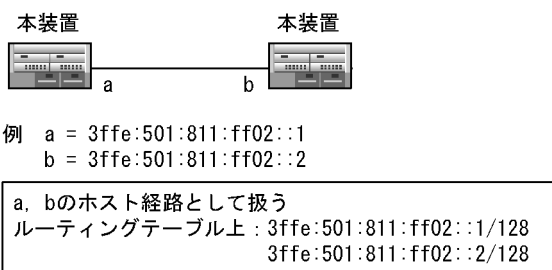
本装置はブロードキャスト型の回線 (イーサネット) とポイント - ポイント型の回線のグローバルアドレスとポイント - ポイント型の回線のリンクローカルアドレスとで経路情報 (直結経路) の扱いが異なります。

(1)　ブロードキャスト型の場合

ブロードキャスト型の場合はネットワークプレフィックス (prefix) とプレフィックス長 (prefixlen) として扱います。ブロードキャスト型の直結経路の扱いを次の図に示します。

図 17-1　直結経路の取り扱い (ブロードキャスト型の場合)

(2)　ポイント - ポイント型のグローバルアドレスおよび手動設定のリンクローカルアドレスの場合

ポイント - ポイント型のグローバルアドレスおよび手動設定のリンクローカルアドレスの場合は，二つのアドレス a，b として扱います。グローバルアドレスおよび手動設定のリンクローカルアドレスの場合の直結経路の扱いを次の図に示します。

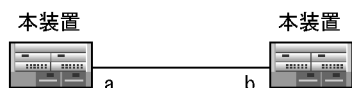
図 17-2　直結経路の取り扱い (ポイント - ポイント型のグローバルアドレス，手動設定リンクローカルアドレスの場合)

(3)　ポイント - ポイント型のリンクローカルアドレスの場合

ポイント - ポイント型のリンクローカルアドレスの場合は，ネットワークプレフィックス（fe80::% 回線

名）とプレフィックス長 (64) として扱います。リンクローカルアドレスの場合の直結経路の扱いを次の図に示します。

図 17-3　ポイント - ポイント型のリンクローカルアドレスの場合

本装置　本装置

a　b

例　prefix/prefixlen=fe80::%回線名/64

サブネット経路として扱う
ルーティングテーブル上：=fe80::%回線名/64

(4) ポイント - ポイント型回線のダイレクト経路の広告

ポイント - ポイント型回線のダイレクト経路 (グローバルアドレスおよび手動設定のリンクローカルアドレス) はホスト経路として生成されます。したがって，ポイント - ポイント型回線のダイレクト経路は二つのホスト経路として広告されます。本装置では，コンフィグレーションコマンド options の gen-prefix-route パラメータを指定することによって，ポイント - ポイント型回線のダイレクト経路を一つのネットワーク経路として広告できます。なお，このパラメータを指定した場合は，該当するダイレクト経路のホスト経路は広告対象外となります。

17.2.3　マルチホーム・ネットワークの設計

マルチホーム接続されたルータで上流プロバイダと経路交換を行う場合は，RIPng ではなく BGP4+ を使用するようにしてください。

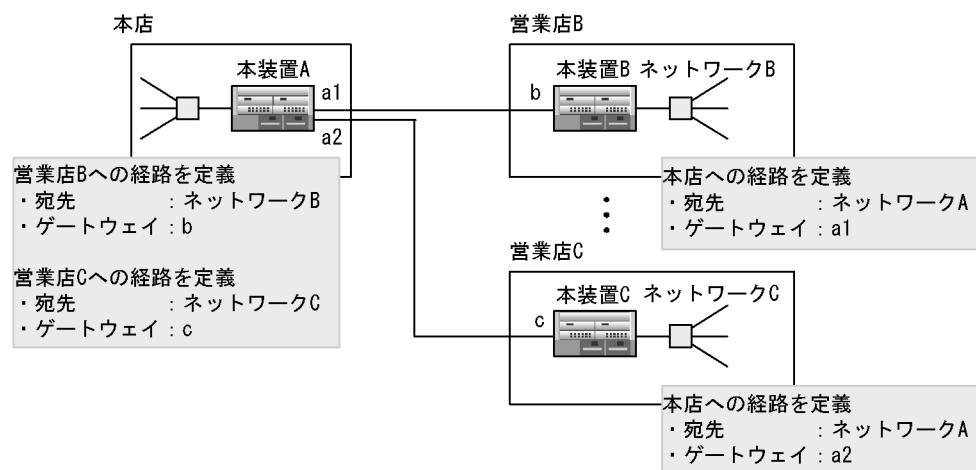
17.3 経路制御 (RIPng/OSPFv3)

17.3.1 スタティックルーティング

スタティックルーティングはコンフィグレーションで設定した経路情報（スタティック経路）に従ってパケットを中継する機能です。

本装置のスタティック経路は，デフォルトルートを含む一つの宛先ネットワークまたはホストごとに，複数の中継経路（ゲートウェイ）を設定できます。本装置は設定された複数の中継経路から適切な一つの経路を選択して経路情報を生成することによってパケット中継を実現しています。

スタティックルーティングのネットワーク構成例を次の図に示します。本店には各営業店へのスタティック経路を定義し，営業店では本店へのスタティック経路を定義します。本設定例では営業店間の通信はできません。

図 17-4　スタティックルーティングのネットワーク構成例

(1) スタティック経路の経路選択

コンフィグレーションで宛先ネットワークごとに指定された複数の中継経路（ゲートウェイ）から適切な一つ，または複数のゲートウェイを選択して経路情報を生成します。ゲートウェイの選択は，該当するゲートウェイと通信できる状態にあるゲートウェイの中からコンフィグレーションの定義順で選択します。

選択されたスタティック経路が使用できなくなった（該当するインタフェースが障害となった）場合，スタティック経路は設定された複数の中継経路から適切な一つ，または複数の経路を再選択します。

本装置では，コンフィグレーションコマンド static の multipath サブコマンドを定義することによって，複数の転送先を生成できます。この複数の転送先（マルチパス）数は，コンフィグレーションコマンド options の max-paths パラメータに従います。

(2) スタティック経路の中継経路指定

スタティック経路では中継経路の指定方法が 3 種類あります。それぞれ，隣接ゲートウェイ，遠隔ゲートウェイ，インタフェースです。

隣接ゲートウェイ

隣接ゲートウェイは，本装置のインタフェースによって直接接続してある装置を中継経路として指定する方法です。該当するゲートウェイへの接続に使用しているインタフェースの状態によって，経路

を生成・削除します。隣接ゲートウェイを指定する場合は，コンフィグレーションコマンド static の gateway サブコマンドを使用してください。

遠隔ゲートウェイ

遠隔ゲートウェイでは，本装置から直接接続していない装置を中継経路として指定できます。該当するゲートウェイへの経路の有無によって，経路を生成・削除します。遠隔ゲートウェイを使用しているスタティック経路のネクストホップは，遠隔ゲートウェイへの経路のネクストホップで置き換えられます。ただし，遠隔ゲートウェイを使用しているスタティック経路を用いて遠隔ゲートウェイを解決することはできません。
遠隔ゲートウェイを指定する場合は，コンフィグレーションコマンド static の remote-gateway サブコマンドを使用してください。

インタフェース

中継経路としてポイント - ポイント型インタフェースを指定することもできます。該当するインタフェースの状態によって，経路を生成・削除します。インタフェース指定のスタティック経路に従ってパケットを転送する場合，そのパケットを該当するインタフェースの対向装置へ転送します。インタフェースを指定する場合は，コンフィグレーションコマンド static の interface サブコマンドを使用してください。

さらに，上記指定の経路について，2 種類のサブコマンドを追加で指定できます。どちらもパケットを転送しないサブコマンドです。また，中継経路に Null インタフェースを指定した場合も，パケットを転送しません。

noinstall サブコマンド

noinstall サブコマンドを指定したスタティック経路はパケット転送に使用しません。デフォルト経路など次善の経路がある場合は，その経路に従ってパケットを転送します。noinstall サブコマンドは，広告用のスタティック経路を設定したいが，パケット転送にはこのスタティック経路を使用しないで，ほかの経路に従ってほしい場合に使用します。

reject サブコマンド

reject サブコマンドを指定したスタティック経路はリジェクト経路になります。その経路にマッチしたパケットは廃棄されます。このとき，ICMP（Unreachable）によって，送信元へパケット廃棄を通知します。reject サブコマンドは，広告用のスタティック経路を設定したいが，このスタティック経路よりも優先する経路が本装置にないパケットを廃棄したい場合に使用します。また，特定のアドレスや宛先に対してパケットを転送したくない場合にも使用します。

Null インタフェース

スタティック経路の中継経路に Null インタフェースを指定すると，結果としてパケットが廃棄されます。また，reject サブコマンドによる廃棄と違い，ICMP を送信しません。パケットを廃棄させたいが，廃棄による ICMP パケットを返したくない場合に使用します。Null インタフェースの詳細は，「16.8　Null インタフェース」を参照してください。

(3) スタティック経路の動的監視

スタティック経路は，ゲートウェイと直接接続されたインタフェースの状態，またはゲートウェイへの経路があるかどうかで経路の生成・削除を制御します。したがって，経路が生成されている場合でも，該当するゲートウェイへの到達保証はありません。本装置では，生成されたスタティック経路のゲートウェイに対し，周期的なポーリングによって，到達性を動的に監視する機能を持っています (コンフィグレーションコマンド static の poll サブコマンド)。本機能を使用することによって，「(2) スタティック経路の中継経路指定」で説明した経路生成・削除条件に加えて，該当するゲートウェイへの到達性が確保できている場合だけ，スタティック経路の生成を制御できます。

17.3.2　ダイナミックルーティング (RIPng/OSPFv3)

本装置では RIPng，OSPFv3，BGP4+，IS-IS をサポートしています。RIPng については「17.4　RIPng」に，OSPFv3 については「17.5　OSPFv3【OP-OSPF(SB-5400S)】」に，BGP4+ については「18　BGP4+【OP-BGP】」を参照してください。IS-IS については「14　IS-IS【OP-ISIS】」を参照してください。

17.3.3　スタティックルーティングとダイナミックルーティングの同時動作 (RIPng/OSPFv3)

スタティックルーティングおよびダイナミックルーティングの各プロトコルは同時に動作できます。

(1)　プリファレンス値

複数のルーティング種別が同時動作するとき，それぞれは独立した経路選択手順に従って，ある宛先アドレスへの経路情報から一つの最良の経路を選択します。その結果，ルータ内ではある宛先アドレスへの経路情報が複数存在することになります。このような場合，それぞれの経路情報のプリファレンス値が比較され優先度の高い経路情報が有効になります。

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコル (例えば RIPng) ごとに生成する経路情報のデフォルトのプリファレンス (優先度) 値をコンフィグレーションで設定できます。なお，プリファレンスは値の小さい方が優先度が高くなります。各プロトコルのプリファレンスのデフォルト値を次の表に示します。

表 17-2　プリファレンスのデフォルト値

経路	デフォルトプリファレンス値
直結経路	0(固定値)
OSPFv3 の AS 内経路	10
IS-IS の内部経路	15
BGP4+ のデフォルト経路	20
スタティック経路	60
RIPng 経路	100
集約経路	130
OSPFv3 の AS 外経路	150
IS-IS の外部経路	160
BGP4+ 経路	170

(2)　エキスポート機能

複数のルーティングプロトコルが同時動作するとき，各ルーティングプロトコルで広告する経路情報は，同一のルーティングプロトコルで学習した経路情報および直結経路情報に限られます。異なるルーティングプロトコルから学習した経路情報は広告されません。例えば，スタティックの経路情報を RIPng では広告しません。また，広告される経路情報はプリファレンス値によって選択された最も優先度の高い経路です。

本装置では，あるルーティングプロトコルの経路情報をほかのルーティングプロトコルで広告したい場合や，特定の経路情報の広告をフィルタリングしたい場合にはエキスポート機能によって実現できます。エキスポートの設定によって広告される経路情報はプリファレンス値から選択された最も優先度の高い経路

です。

(a) OSPFv3 ドメインの注意事項

OSPFv3 の各ドメインは，お互いに異なるルーティングプロトコルとして動作します。このため，エキスポート機能を使用しない場合，ルータ内の複数の OSPFv3 ドメイン間でお互いに経路を広告することはありません。OSPFv3 の AS 内経路や AS 外経路をほかの OSPFv3 ドメインに AS 外経路として広告したい場合には，配布先ドメインに対してエキスポート・フィルタを定義してください。

17.3.4 経路削除保留機能

経路削除保留機能は，ルーティングプロトコルが無効にした経路を，ルーティングテーブルから一定時間削除しないようにすることで，新しく代替経路が生成されるまでの間，既存経路によってフォワーディングを維持する機能です。

経路削除保留機能については，「13.2.4　経路削除保留機能」を参照してください。

17.4 RIPng

17.4.1 RIPng 概説

RIPng はネットワークで接続したルータ間で使用するルーティングプロトコルです。各ルータは RIPng を使用して自ルータから到達できるネットワークとそのネットワークへのホップ数 (メトリック) を通知し合うことによって経路情報を生成します。RIPng はバージョン 1(RFC2080 準拠) をサポートしています。

(1) メッセージの種類

RIPng で使用するメッセージの種類にはリクエストとレスポンスの 2 種類があります。ルータがほかのルータに経路情報を要求する場合にはリクエストを使用し，ほかのルータからのリクエストに応答する場合，および定期的またはトポロジー変化時に自ルータの経路情報をほかのルータに通知する場合にレスポンスを使用します。

(2) 運用時の処理

本装置の立ち上げ時，本装置はリクエストメッセージをすべての隣接ルータに送信し，隣接ルータが持つすべての経路情報を通知するように要求します。

運用中，本装置は次の三つの要因でレスポンスを送信します。

- 隣接ルータからリクエストを受信した場合で，リクエストの内容によって自分が持つ経路情報をリクエストの送信元にレスポンスで応答します。
- 定期的に行う経路情報の通知です。本装置は 30 秒ごとに自分が持つ経路情報をすべて含むレスポンスを送信し，隣接ルータに通知します。
- 経路変化を検出したときに行う経路情報の通知です。本装置は経路の変化を検出したとき，変化した経路に関連する経路情報を含むレスポンスを送信し，隣接ルータに通知します。

各隣接ルータが送信したレスポンスを受信し，経路の変更を検出した場合は自分が持つ経路情報の更新を行います。レスポンスは隣接ルータとの送信の確認にも使用します。180 秒以上レスポンスを応答しないルータに対しては通信不可能と判断し，代替ルートがあるときはルーティングテーブルを代替ルートに更新します。代替ルートがないときはルートを削除します。

(3) ルーティングループの抑止処理

本装置は中継経路のループを抑止するためにスプリットホライズンを使用します。

(4) RIPng(IPv6) と RIP(IPv4) の機能差分

RIPng(IPv6) と RIP(IPv4) の機能差分を次の表に示します。

表 17-3 RIPng(IPv6) と RIP(IPv4) の機能差分

機能	RIPng(IPv6)	RIP(IPv4)
triggered update	○	○
ホールドダウン	○	○
スプリットホライズン	○	○
ポイズンリバース	×	×
認証機能	×	×

機能	RIPng(IPv6)	RIP(IPv4)
ルートタグ	○※	△
指定ネクストホップの取り込み	○	○
既存経路と同じメトリックの経路を異なるゲートウェイから受信したときに，既存経路のエージングタイムがタイマ値の 1/2 秒以上経過している場合，新しく学習した経路に変更します。	×	○

（凡例） ○：取り扱う　△：一部取り扱う　×：取り扱わない

注※　ルートタグ情報の変更はサポートしていません。

17.4.2　経路選択アルゴリズム経路集約

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同じ宛先への経路情報が各プロトコルで生成されて複数存在する場合，それぞれの経路情報のプリファレンス値が比較され優先度の最も高い経路情報が有効になります。

RIPng では，自プロトコルを使用し学習した同じ宛先への広告元の異なる複数の経路情報から，経路選択の優先順位に従って一つの最良の経路を選択します。

表 17-4　経路選択の優先順位

優先順位	内容
高	メトリック値が最も小さい経路を選択します。
↑	ネクストホップアドレスが最も小さい経路を選択します。
↓	経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。※
低	そのほかの場合，新しく学習した経路を無視します。

注※　この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。

その後，同じ宛先への経路情報が各プロトコル（BGP4+，スタティック）で学習した経路によって複数存在する場合は，それぞれの経路情報のプリファレンス値が比較され，優先度の最も高い経路情報をルーティングテーブルに設定します。

17.4.3　RIPng での経路情報の広告

ルーティングプロトコルに RIPng(RFC2080 準拠）を使用する場合は経路情報の伝搬に注意が必要です。経路情報の種類を次の表に示します。

表 17-5　経路情報の種類

経路情報の種類	定義	例
デフォルト経路情報	すべてのネットワーク宛ての経路情報	::/0
ネットワーク経路情報	特定のネットワーク宛てのグローバル経路情報	3ffe:501:811:ff01::1/64 3ffe:501:811:ff::/52 fec0::/64
ホスト経路情報	特定のホスト宛てのグローバル経路情報（ポイント - ポイント型回線の経路情報も含みます）	3ffe:501:811:ff01:8ff:fe8e:3090/128 fec0::1/128

（1）IPv6 インタフェースが一つの場合の RIPng 広告について

本装置ではインタフェースがアップしていて通信できる状態の IPv6 インタフェースが一つの場合でも，RIPng 広告を行います。IPv6 インタフェースが一つの場合で RIPng による通信を停止したいときには，コンフィグレーションによって RIPng の動作を停止してください。

17.4.4 RIPng の機能

RIPng は広告する経路情報に該当する経路のプレフィックス長を設定するため，可変プレフィックス長を取り扱うことができます。RIPng の機能を次に示します。

- 認証機能
  本装置では認証機能をサポートしていません。
- ルートタグ
  本装置ではレスポンスメッセージで通知された経路情報のルートタグ情報が設定されている場合，ルーティングテーブルにルートタグ情報を取り込みます。本装置から通知するレスポンスメッセージの経路情報のルートタグ情報はルーティングテーブルの該当する経路のルートタグを設定します。なお，使用できる範囲は 1 ～ 255(10 進数) です。
  また，RIPng ではインポート・フィルタでのルートタグ情報によるフィルタリング，およびエキスポート・フィルタ (そのほかのプロトコルから RIPng に経路を配布する) でのルートタグ情報の変更はサポートしていません。
- プレフィックス
  本装置では，レスポンスメッセージで通知された経路情報のプレフィックス長をルーティングテーブルに取り込みます。本装置から通知するレスポンスメッセージの経路情報のプレフィックス長は，ルーティングテーブルの該当する経路のプレフィックス長を設定します。
- ネクストホップ
  本装置ではレスポンスメッセージで通知された経路情報のネクストホップ情報が設定されている場合，ルーティングテーブルに該当するネクストホップ情報を取り込みます。ネクストホップ情報が設定されていない場合，送信元のゲートウェイをネクストホップとして認識します。
  本装置から通知するレスポンスメッセージでは経路情報のネクストホップ情報を設定しません。そのため本装置から RIPng で経路を受信したルータは，送信インタフェースのインタフェースアドレスをネクストホップとして使用します。
- リンクローカルマルチキャストアドレスの使用
  本装置では RIPng メッセージを受信しないホストでの不要な負荷を軽減するために，リンクローカルマルチキャストアドレスをサポートします。RIPng メッセージの送信時に使用するリンクローカルマルチキャストアドレスは，全 RIPng ルータマルチキャストアドレス (ff02::9) です。

17.4.5 RIPng による経路広告／切り替えのタイミング

RIPng による経路広告／切り替えのタイミングは，RIPng が持つ次の四つの機能が関係します。

1. 周期的な経路情報広告
2. エージングタイムアウト
3. triggered update
4. ホールドダウン

各機能で使用する RIPng タイマを次の表に示します。

表 17-6　RIPng タイマ

タイマ名称	タイマ値	内容
周期広告タイマ※1※2	30 秒 (デフォルト)	自ルータが持つ経路情報を隣接ルータに周期的に通知するために使用します。
エージングタイマ※2	180 秒 (デフォルト)	隣接ルータから通知された経路情報の周期的な通知が一定時間ない場合に経路情報を削除するために使用します。
triggered update	なし (経路変動が発生したとき)	自装置の経路情報の変化を認識したときに定期的な配布周期を待たないで経路情報を配布します。
ホールドダウンタイマ※2	120 秒 (デフォルト)	経路情報が削除されたことを隣接ルータに一定時間通知するために使用します。

注※ 1

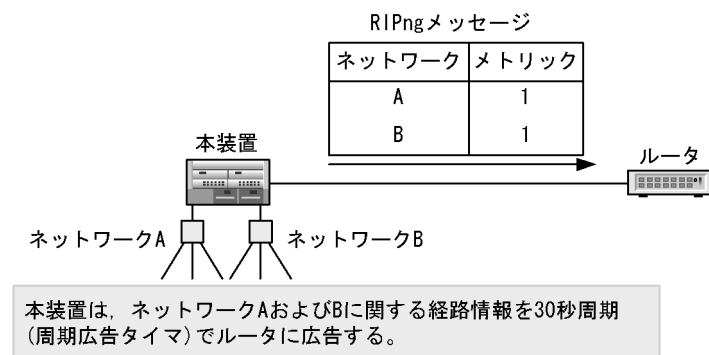
指定タイマ値 (デフォルト : 30 秒) の± 50%(デフォルト : 15 ～ 45 秒) の範囲で動的に変動します。

注※ 2

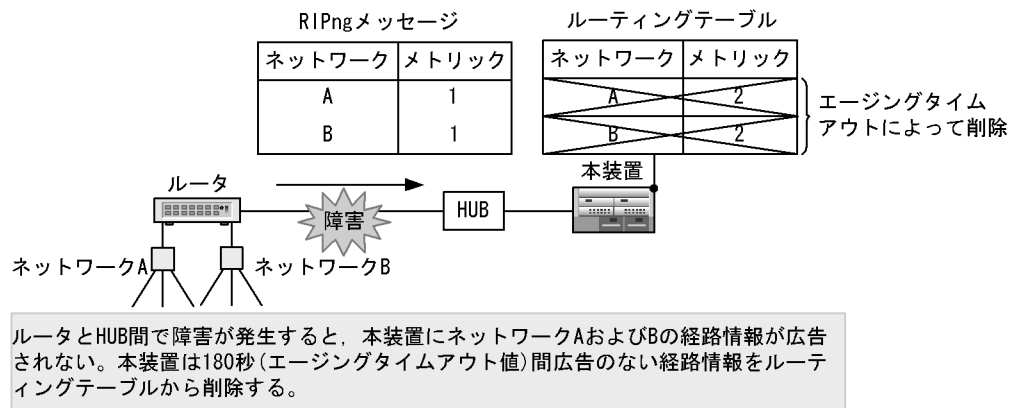
コンフィグレーションで変更できます。

(1) 周期的な経路情報広告

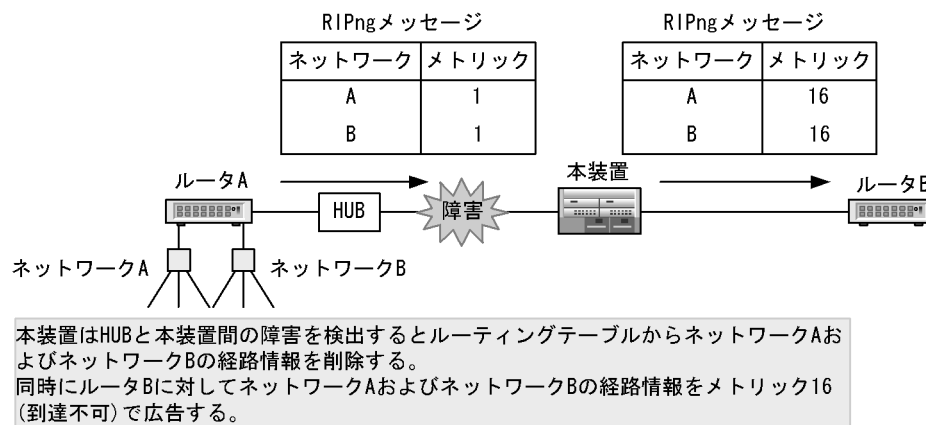
RIPng は自装置が持つすべての経路情報を周期的に隣接のルータに広告します。周期的な経路情報の広告を次の図に示します。

図 17-5　周期的な経路情報の広告

(2) エージングタイムアウト

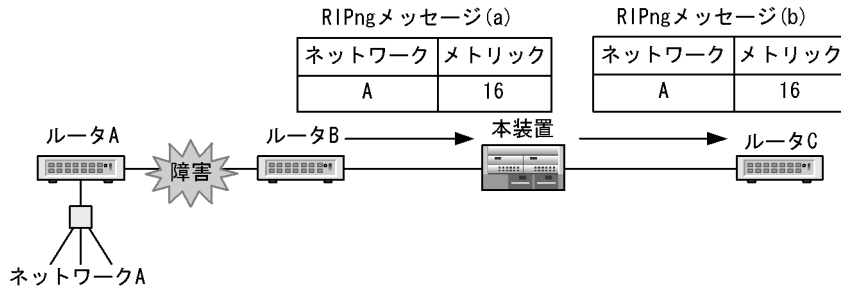
RIPng は隣接から受信した経路情報が最良の経路の場合，自装置のルーティングテーブルに取り込みます。取り込んだ経路情報はエージングタイマによって監視されます。エージングタイマは隣接からの周期的な広告によってリセット (クリア) します。隣接装置の障害や自装置と隣接装置間の回線障害などによって，隣接から該当する経路情報の広告が 180 秒 (エージングタイムアウト値) 間ない場合，該当する経路情報を自装置のルーティングテーブルから削除します。エージングタイムアウトによる経路情報の削除を次の図に示します。

図 17-6　エージングタイムアウトによる経路情報の削除

（3） triggered update

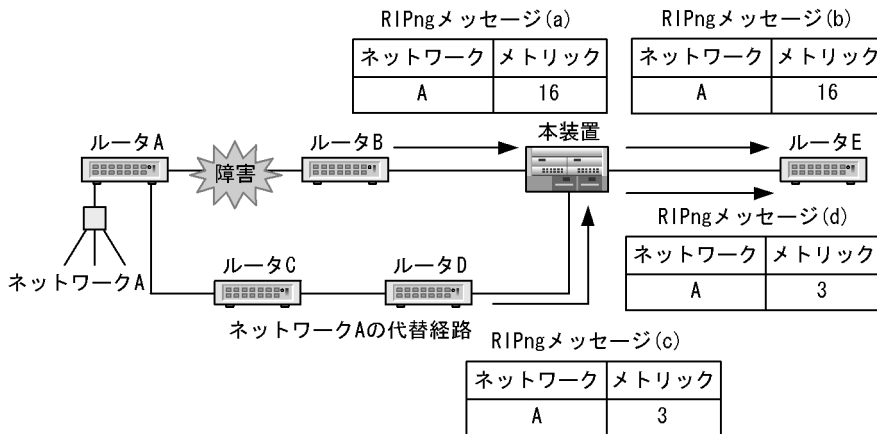
自装置の経路情報の変化を認識したときに定期的な配布周期を待たないで経路情報を配布します。triggered update による経路情報の広告を次の図に示します。

図 17-7　triggered update による経路情報の広告

（4） ホールドダウン

到達可状態から到達不可状態（メトリック 16 受信，またはインタフェース障害によって該当するインタフェースから学習した経路を削除）となった経路に対して，一定時間（120 秒：ホールドダウンタイマ）はメトリック 16(到達不可）で隣接ルータに広告します。ホールドダウンタイマは古くなったメッセージを誤って受け取ることのないように十分な時間になっています。ホールドダウンを次の図に示します。

図 17-8 ホールドダウン

(a) 本装置はルータAとルータB間の障害を検出するとルータBからメトリック16(到達不可)のネットワークAの経路情報を受信し，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) (a)を受信して即時に，本装置はルータCにメトリック16(到達不可)のネットワークAの経路情報を広告する。本装置は代替経路が存在しない場合，ホールドダウン時間(メトリック受信後，120秒間)は該当経路をメトリック16(到達不可)でルータCに広告する。

ホールドダウン期間中に，該当する宛先への新しい経路を再学習した場合は，ホールドダウンタイマを停止し，新しい経路を広告します。ホールドダウン期間中の再学習を次の図に示します。

図 17-9 ホールドダウン期間中の再学習

(a) 本装置はルータAとルータB間の障害を検出するとルータBからメトリック16(到達不可)のネットワークAの経路情報を受信し，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) 同時に本装置はルータEにメトリック16(到達不可)のネットワークAの経路情報を広告する。
(c) 本装置はルータDからの周期広告でネットワークAの経路情報を受信し，ルーティングテーブルに追加する(切り替え時間はルータDの周期広告時間による)。
(d) 本装置はホールドダウンタイマを停止し，ルータEに対してネットワークAの経路情報を広告する。

17.4.6 高速経路切替機能

(1) 概要

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報（第1優先経路と呼ぶ）と，第1優先経路の次に優先される経路（第2優先経路と呼ぶ）をあらかじめルーティングテーブルに登録しておき，インタフェースダウンによって，第1優先経路が使用不可能になったとき，素早く第2優先経路をフォワーディング・テーブルに登録することによって通信停止時間の短縮を図る機能です。

高速経路切替機能の詳細については「18.2.5　高速経路切替機能」を参照してください。

(2) 第 2 優先経路の生成

コンフィグレーションコマンド options の fast-reroute パラメータおよびコンフィグレーションコマンド rip の fast-reroute サブコマンドの gen-secondary-route パラメータ，または gen-secondary-route サブコマンドを指定することによって，異なる隣接装置から学習した同一宛先への経路情報を二つ（第 1 優先経路と第 2 優先経路）まで生成します。RIPng では高速経路切替機能用に第 2 優先経路を生成する指定と，高速経路切替機能を使用せずに第 2 優先経路を生成する指定ができます。第 2 優先経路を生成する条件を次の表に示します。

表 17-7　第 2 優先経路の生成条件

条件				第 2 優先経路の生成
コンフィグレーションコマンド options の fast-reroute パラメータ	コンフィグレーションコマンド ripng の fast-reroute サブコマンドの gen-secondary-route パラメータ	コンフィグレーションコマンド ripng の gen-secondary-route サブコマンド	プリファレンス値	
×	-	-	-	生成しない
○	×	-	-	生成しない
○	○	-	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
○	○	-	第 1 優先経路と第 2 優先経路の値が同じ	生成する
-	-	×	-	生成しない
-	-	○	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
-	-	○	第 1 優先経路と第 2 優先経路の値が同じ	生成する

（凡例）　○：コンフィグレーションあり　×：コンフィグレーションなし　-：対象外

注　コンフィグレーションコマンド options の fast-reroute パラメータとコンフィグレーションコマンド ripng の gen-secondary-route サブコマンドは同時に指定できません。

第 2 優先経路の生成を指定した場合，次の表に従って同じ宛先への経路情報の優先度を決定します。

表 17-8　第 2 優先経路の登録を指定した場合の経路選択の優先順位

優先順位	内容
高	メトリック値が小さい経路を選択します。
↑	ネクストホップアドレスが小さい経路を選択します。※1
	経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。※2
↓	ネクストホップが同じ，かつネクストホップアドレスと送信元ゲートウェイアドレスが同じ経路がない場合，今まで第 1 優先であった経路を選択します。

優先順位	内容
低	そのほかの場合，新しく学習した経路を無視します。

注
　ネクストホップアドレスが同じ場合は第 1 優先経路だけ生成します。

注※ 1
　第 2 優先経路が登録されている状態で新経路を学習した場合，この条件は適用されません。

注※ 2
　この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。

17.4.7 RIPng 使用時の注意事項

RIPng を使用したネットワークを構成する場合には次の制限事項に留意してください。

(1) RIPng の制限事項

本装置は RFC2080(RIPng バージョン 1) に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 17-9　RFC との差分

RFC		本装置
must be zero フィールド	処理については特に明記されていません。	本装置では，must be zero フィールドの値をチェックしません。また，送信時には，must be zero フィールドを 0 にします。
ネットワークプレフィックス	プレフィックス長以降のアドレスフィールドの状態については特に明記されていません。	受信した RIPng パケットで，プレフィックス長以降のアドレスフィールドが 0 クリアされていない経路情報を受信したときはプレフィックス長以降のアドレスは 0 クリアします。
triggered update	triggered update 後，1 〜 5 秒のランダムタイマを設定するべきであり，タイムアウト前にアップデートを送信する変更があっても，タイムアウトした際にアップデートを行います。	triggerd update 後に 1 〜 5 秒のランダムタイマは設定せず，経路情報に変更があった際は随時 triggered update を行います。
	triggered update 後の 1 〜 5 秒のランダムタイマ起動中に通常のアップデートがある場合，triggered update は抑止されるかもしれません。	triggered update の抑止は行いません。
スプリットホライズン	スプリットホライズン機能はインタフェース単位で設定変更を可能とするべきです。	本装置ではスプリットホライズン機能のインタフェース単位で設定変更はサポートしていません。
タグ値の割り当て方	具体的な規則は明記されていません。	本装置では受信したタグ値を流用します。タグ値が定義されていない場合は，固定値か BGP4+ 経路のピア AS 番号かを割り当てます。どちらを割り当てるかはコンフィグレーションによって変更できます。
経路のネクストホップ情報指定	経路のネクストホップを明示的に指定できます。	本装置から送信する RIPng パケットにはネクストホップ情報は含まれません。本装置がネクストホップ情報を明示的に指定した RIPng パケットを受信した場合は，その値をネクストホップとして採用します。

RFC		本装置
応答パケットの 送信先	ff02::9 宛てでは不適切な場合（例.NBMA ネットワーク）については実装依存とします。	本装置では，NBMA ネットワークでの RIPng 動作はサポートしていません。
送信先・受信元 ルータの制限	実装上指定できることが望ましいです。	本装置では，送信先・受信元ルータを明示的に制限できません。
認証	IPv6 認証ヘッダおよび暗号化ヘッダを使用してパケットを認証します。	本装置では IPv6 認証ヘッダ，暗号化ヘッダによるパケット認証はサポートしていません。
送信元ポート 521 以外のユニキャストによるリクエストパケット受信時のレスポンスパケット返送	送信元アドレスに対して直接返送することができます。	本装置では，送信元アドレスにリンクローカルアドレスを指定したリクエストパケットに対してだけレスポンスパケットを返送します。

17.5 OSPFv3【OP-OSPF(SB-5400S)】

17.5.1 OSPFv3 概説

OSPFv3 はルータ間の接続状態から構成されるトポロジと Dijkstra アルゴリズムによる最短経路計算に基づく IPv6 用のルーティングプロトコルです。ルータ ID とエリア ID は OSPF(IPv4) と同様 32 ビット数です。OSPF と OSPFv3 はそれぞれ独立して動作します。

(1) OSPFv3 の特長

OSPFv3 は，通常一つの AS 内での経路決定に使用されます。OSPFv3 では，AS 内のすべての接続状態から構成するトポロジのデータベースが各ルータにあり，このデータベースに基づいて最短経路を計算します。このため，OSPFv3 は RIPng と比較して，次に示す特長があります。

- 経路情報トラフィックの削減
  OSPFv3 では，ルータ間の接続状態が変化したときだけ，接続状態の情報をほかのルータに通知します。このため，OSPFv3 は RIPng のように定期的にすべての経路情報を通知するルーティングプロトコルと比較して，ルーティングプロトコルが占有するトラフィックが小さくなります。なお，OSPFv3 では 30 分周期で，自ルータの接続状態の情報を他ルータに通知します。
- ルーティングループの抑止
  OSPFv3 を使用しているすべてのルータは，同じデータから成るデータベースを保持しています。各ルータは共通のデータに基づいて経路を選択します。したがって，RIPng のようなルーティングループ (中継経路の循環) は発生しません。
- コストに基づく経路選択
  OSPFv3 では，宛先まで到達できる経路が複数存在する場合，宛先までの経路上のコストの合計が最も小さい経路を選択します。これによって，RIPng と異なり経路へのコストを柔軟に設定できるため，中継段数に関係なく望ましい経路を選択できます。
- 大規模なネットワークの運用
  OSPFv3 では，コストの合計が 16,777,214 以内の経路を扱えます。このため，メトリックが 1 〜 15 までの範囲である RIPng と比較して，より大規模で経由ルータ数の多い経路が存在するネットワークの運用に適しています。

(2) OSPFv3 と OSPF との機能差分

OSPFv3(IPv6) と OSPF(IPv4) との機能差分を次の表に示します。

表 17-10 OSPFv3(IPv6) と OSPF(IPv4) の機能差分

機能	OSPFv3(IPv6)	OSPF(IPv4)
ポイント・ポイント型インタフェースのアドレス広告	自側アドレスをコスト 0 で広告 ※1	相手側アドレスを指定コストで広告
AS 外経路のフォワーディングアドレス	×	○
NSSA	×	○
認証	×	○
非ブロードキャスト (NBMA) ネットワーク	×	○
イコールコストマルチパス	○※2	○
仮想リンク	○※3	○

機能	OSPFv3(IPv6)	OSPF(IPv4)
マルチバックボーン	○	○
グレースフル・リスタート	○※4	○※4

(凡例)　○：取り扱う　×：取り扱わない

注※1

コンフィグレーションコマンド options の gen-prefix-route パラメータを指定した場合，プレフィックス長が 128 でないポイント - ポイント型インタフェースについてはネットワーク経路を指定コストで広告します。このとき自側アドレスは仮想リンクで必要なければ広告しません。

注※2

経路選択方法は，OSPF(IPv4) と OSPFv3(IPv6) で異なります。イコールコスト時，OSPF(IPv4) では最小のネクストホップアドレスを選択しますが，OSPFv3(IPv6) ではルータ ID が最小であるネクストホップアドレスを選択します。同一ルータ ID のネクストホップアドレスが複数ある場合，Hello パケットで最小のインタフェース ID を広告しているネクストホップアドレスを選択します。

注※3

仮想リンクの設定には，通過エリア上のインタフェースに IPv6 グローバルまたは IPv6 サイトローカルアドレスを設定しておく必要があります。

注※4

SB-5400S ではヘルパー機能だけサポートします。

17.5.2　経路選択アルゴリズム

OSPFv3 では，経路選択のアルゴリズムとして，SPF(Shortest Path First) アルゴリズムを使用します。各ルータには，OSPFv3 が動作しているすべてのルータと，ルータ - ルータ間およびルータ - ネットワーク間のすべての接続から成るデータベースがあります。このデータベースから，ルータおよびネットワークを頂点とし，ルータ - ルータ間およびルータ - ネットワーク間の接続を辺とするトポロジを構成します。このトポロジに SPF アルゴリズムを適用して最短経路木を生成し，これを基に各頂点への経路を決定します。

(1)　SPF アルゴリズムの適用例

ネットワーク構成の例を次の図に示します。

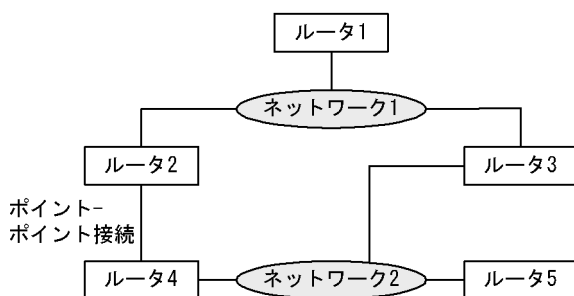
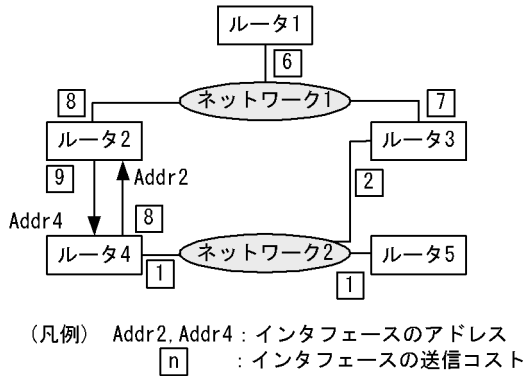
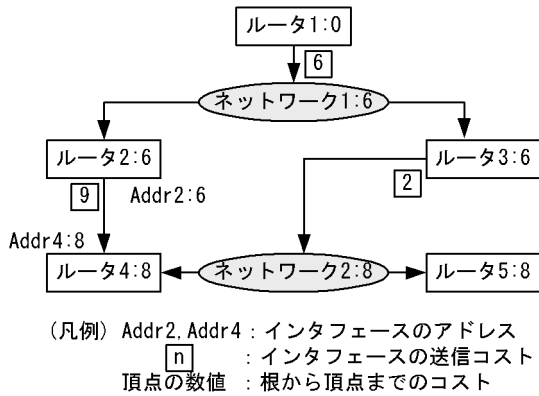
図 17-10　ネットワーク構成例

この図のネットワーク上で OSPFv3 を使用した場合のトポロジとコストの設定例を次の図に示します。

図 17-11　トポロジとコストの設定例

コスト値は，パケット送信方向により異なってもかまいません。「図 17-11　トポロジとコストの設定例」のルータ 2- ルータ 4 間のポイント - ポイント型接続では，ルータ 2 からルータ 4 へはコスト 9，ルータ 4 からルータ 2 へはコスト 8 となっています。ルータ - ネットワーク間の接続では，ルータからネットワークへの接続だけ，コストを設定できます。ネットワークからルータへのコストは常に 0 です。

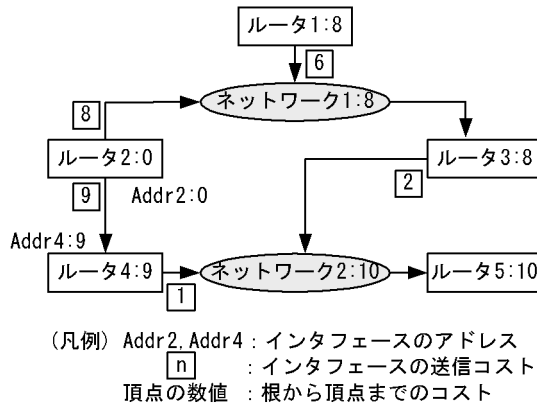
「図 17-11　トポロジとコストの設定例」のトポロジを基に，ルータ 1 を根として生成した最短経路木を「図 17-12　ルータ 1 を根とする最短木」に示します。ある宛先へのコストは，経路が経由す各インタフェースの送信コストの合計となります。例えば，ルータ 1 からネットワーク 2 宛ての経路のコストは，6(ルータ 1- ネットワーク 1) ＋ 0(ネットワーク 1- ルータ 3) ＋ 2(ルータ 3- ネットワーク 2) ＝ 8 となります。

図 17-12　ルータ 1 を根とする最短木

(a)　ルータ ID，ネットワークアドレスについての注意事項

OSPFv3 ではネットワークのトポロジを構築するに当たり，ルータの識別にルータ ID を使用します。したがって，ネットワークの設計時に異なるルータに同じ値のルータ ID を定義した場合，正確な経路選択ができなくなります。このためネットワーク設計時には，各ルータに重複しないルータ ID を割り当ててください。

(2)　イコールコストマルチパス

ルータ 2 を根として生成した最短経路木を「図 17-13　ルータ 2 を根とする最短木」に示します。ネットワーク 2 またはルータ 5 を宛先とした場合，ネットワーク 1 経由の経路とルータ 4 経由の経路については，コストが同じになります。

図 17-13　ルータ 2 を根とする最短木

OSPFv3 では，ある 2 点間に最短コストの経路が複数存在する場合，この複数の経路をイコールコストマルチパスと呼びます。

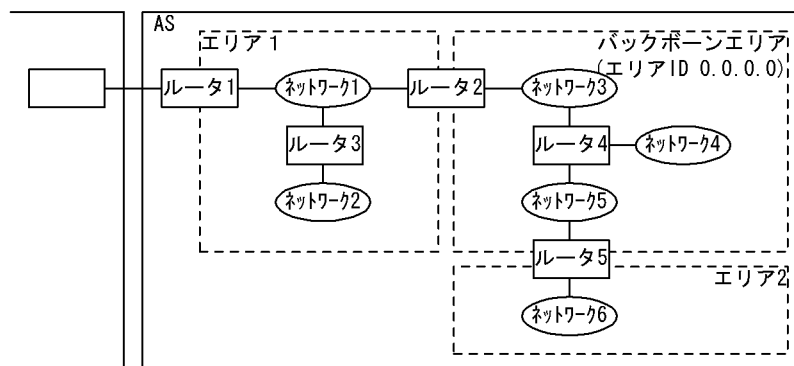
OSPFv3 では，自ルータからある宛先についてイコールコストマルチパスが存在し，次の転送先ルータが複数ある場合，その宛先へのパケットの転送を複数のネクストホップへ分散することによって，トラフィックを分散してもよいことになっています。

本装置では，コンフィグレーションコマンド ospf6 の multipath サブコマンドを定義することによって，複数のネクストホップを生成できます。この複数のネクストホップ (マルチパス) 数は，コンフィグレーションコマンド options の max-paths パラメータに従います。multipath サブコマンドを定義しなかった場合，ルータ ID が最小であるネクストホップアドレスを選択します。同一ルータ ID のネクストホップアドレスが複数ある場合，Hello パケットで最小のインタフェース ID を広告しているネクストホップアドレスを選択します。

17.5.3　エリア分割

OSPFv3 では，ルーティングに必要なトラフィックと，経路選択に使用するアルゴリズムの処理に必要な時間を削減するために，AS を複数のエリアに分割できます。

エリア分割を使用した OSPFv3 ネットワークトポロジの例を次の図に示します。

図 17-14　エリア分割を使用した OSPFv3 ネットワークトポロジの例

あるエリア内の接続状態の情報は，ほかのエリアには通知されません。また，ルータには，接続していないエリアの接続状態の情報はありません。

(1) バックボーン

エリア ID が 0.0.0.0 であるエリアをバックボーンと呼びます。AS が複数のエリアに分割されている場合，バックボーンには特別な役割があります。AS を複数のエリアに分割する場合には，エリアのどれか一つをバックボーンエリアとして定義する必要があります。ただし，一つの AS にバックボーンを二つ以上ある構成にしないでください。そのような構成の場合，情報がそれぞれのバックボーンに分散されるため，到達不能である経路が発生したり，最適な経路を選択しなかったりすることがあります。

(2) エリアボーダルータ

「図 17-14　エリア分割を使用した OSPFv3 ネットワークトポロジの例」のルータ 2 やルータ 5 のように，複数のエリアに所属するルータを，エリアボーダルータと呼びます。エリアボーダルータでは，所属しているすべてのエリアについて，それぞれ別個に SPF アルゴリズムに基づいて経路選択を行います。なお，エリアボーダルータは，バックボーンを通じてエリア間の経路情報の交換を行うため，必ずバックボーンに所属する必要があります。

(a) エリア分割についての注意事項

エリア分割を行うと，ルータや経路情報トラフィックの負荷が減る一方で，OSPFv3 のアルゴリズムが複雑になります。特に，障害に対して適切な動作をする構成が困難になります。ルータやネットワークの負荷に問題がない場合は，エリア分割を行わないことをお勧めします。

(b) エリアボーダルータについての注意事項

- エリアボーダルータでは，所属しているエリアの数だけ SPF アルゴリズムを動作させます。エリアボーダルータには，あるエリアのトポロジ情報を要約し，ほかのエリアへ通知する機能があります。このため，所属するエリアの数が多くなるとエリアボーダルータの負荷が高くなります。このため，エリアボーダルータにあまり多くのエリアを所属させないようなネットワーク構成にすることをお勧めします。
- あるエリアにエリアボーダルータが一つしかない場合，このエリアボーダルータに障害が発生すると，バックボーンから切り放され，ほかのエリアとの接続性が失われます。重要な機能を提供するサーバや重要な接続のある AS 境界ルータの存在するエリアには，複数のエリアボーダルータを配置し，エリアボーダルータの配置に対して十分な迂回路が存在するように，ネットワークを構築することをお勧めします。
- インタフェースおよび装置アドレスを同時に複数のエリアの OSPFv3 インタフェースとなる構成にしないでください。本装置に接続している各インタフェースおよび装置アドレスは，それぞれ一つのエリアだけに所属できます。複数のエリアに OSPFv3 インタフェースとして定義した場合，対象インタフェースおよび装置アドレスは，どのエリアでも OSPFv3 インタフェースとして動作しなくなります。

(3) スタブエリア

バックボーンではなく，AS 境界ルータが存在しないエリアをスタブエリアとして定義 (コンフィグレーションコマンド area(ospf6 モード) の stub サブコマンドで指定) できます。

エリアボーダルータは，スタブエリアとして定義したエリアに AS 外経路を導入しません。このため，スタブエリア内では経路情報を減らし，ルータの情報の交換や経路選択の負荷を減らすことができます。

AS 外経路の代わりとして，スタブエリアにデフォルトルートを導入するようにエリアボーダルータを設定 (コンフィグレーションコマンド area(ospf6 モード) の stub cost サブコマンドで指定) できます。この設定によって，スタブエリア内の AS 外経路の扱いについては，デフォルトルートへのコストとエリアボーダルータまでのコストの合計に基づいて，経路を選択します。ただし，デフォルトルートに基づいて経路が選択されるため，スタブエリア内では，AS 外経路について比較的遠い経路を選択することがあります。

(4) エリア分割した場合の経路制御

エリアボーダルータは，バックボーンを除くすべての所属しているエリアの経路情報を要約した上で，バックボーンに所属するすべてのルータへ通知します。また，バックボーンの経路情報の要約と，バックボーンに流れている要約されたほかのエリアの経路情報を，バックボーン以外の接続しているエリアのルータへ通知します。

あるルータが，あるアドレスについて，要約された経路情報を基に経路を決定した場合，このアドレス宛ての経路は要約された経路情報の通知元であるエリアボーダルータを経由します。このため，異なるエリア間を結ぶ経路は必ずバックボーンを経由します。

(5) エリアボーダルータでの経路の要約

エリアボーダルータでは，あるエリアの経路情報をほかのエリアに広告するに当たってルータやネットワーク間の接続状態と接続のコストによるトポロジ情報を，エリアボーダルータからルータやネットワークへのコストに要約します。

経路の集約および抑制とエリア外への要約を次の表に示します。

表 17-11　経路の集約および抑制とエリア外への要約

エリア内のネットワークアドレス	集約および抑制の設定	エリア外へ通知する要約
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60	なし	3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60	3ffe:501:811::/59 3ffe:501:811::20::/60	3ffe:501:811::/59 3ffe:501:811:20::/60 3ffe:501:811:30::/60
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60 3ffe:501:811:ff00::/58	3ffe:501:811::/58(抑制) 3ffe:501:811:ff00::/56	3ffe:501:811:ff00::/56

エリアボーダルータでのエリア内のトポロジ情報を要約するに当たり，アドレスの範囲を定義することによって，その範囲に含まれる経路情報を一つに集約できます。アドレスの範囲の指定には，プレフィックス長指定のあるプレフィックスを使用します (コンフィグレーションコマンド area(ospf6 モード) の networks サブコマンドで指定)。

集約する範囲を定義すると，エリア内に定義したプレフィックスの範囲に含まれるネットワークが一つでもあった場合，範囲に含まれるすべてのネットワークをこのプレフィックスを宛先とする経路情報へ集約し，ほかのエリアへ通知します。範囲に含まれる各ネットワークは，このエリアボーダルータからほかのエリアへは通知されません。このとき，集約した経路情報のコストには範囲に含まれるネットワーク中の最も大きなコストを使用します。

また，このプレフィックスの範囲に含まれるネットワークの広告を抑制 (コンフィグレーションコマンド area(ospf6 モード) の networks サブコマンドで restrict を指定) できます。この場合，範囲内の各ネットワークをほかのエリアへは通知しない上に，プレフィックスに集約した経路もほかのエリアへは通知しません。この結果，ほかのエリアからはこのエリアボーダルータ経由で指定した範囲に含まれるアドレスへの経路は存在しないように見えます。

集約および抑止するアドレスの範囲は，一つのエリアについて複数定義できます。また，エリア内にどの定義の範囲にも含まれないアドレスを使用しているルータやネットワークが存在してもかまいません。ただし，ネットワークを構成するに当たり，トポロジと合ったアドレスを割り当てた上で，トポロジに応じ

た範囲を使用して集約を定義すると，選択する経路の適切さを損なわないで，効率的に OSPFv3 の経路情報トラフィックを削減できます。

(6) 仮想リンク

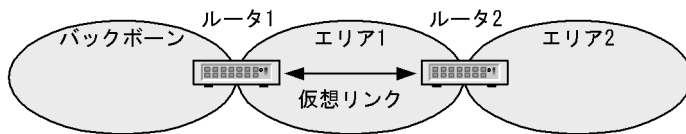
OSPFv3 では，スタブエリアとして定義しておらず，バックボーンでもないエリア上のある二つのエリアボーダルータで，このエリア上の二つのルータ間の経路をポイント - ポイント型回線と仮想することによって，バックボーンのインタフェースとして使用できます。この仮想の回線のことを**仮想リンク**と呼びます。仮想リンクの実際の経路があるエリアのことを，仮想リンクの通過エリアと呼びます。仮想リンクの隣接ルータとの通信には，IPv6 グローバルまたは IPv6 サイトローカルアドレスを使用します。このアドレスは，通過エリアに属した任意のインタフェース上の IPv6 グローバルまたは IPv6 サイトローカルアドレスを使用します。このインタフェースの IPv6 アドレスは，仮想リンクの隣接ルータが OSPFv3 パケットの宛先アドレスとして使用します。

仮想リンクの使い方として，次に示す三つの例を挙げます。

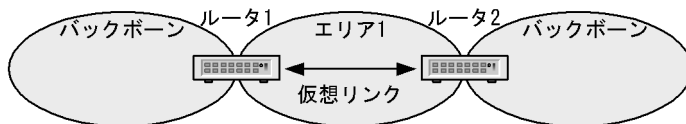
- バックボーンに物理的に接続していないエリアの仮想接続
- 複数のバックボーンの結合
- バックボーンの障害による分断に対する経路の予備

(a) バックボーンに物理的に接続していないエリアの仮想接続

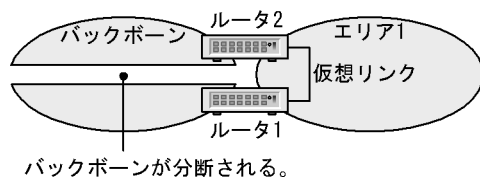
次の図で，エリア 2 はバックボーンに接続していません。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義することによって，ルータ 2 はバックボーンに接続するエリアボーダルータとなり，エリア 2 をバックボーンに接続していると見なせるようになります。

図 17-15　エリアのバックボーンへの接続

(b) 複数のバックボーンの結合

次の図では，AS 内にバックボーンであるエリアが二つ存在します。この状態では，バックボーンの分断による経路到達不能などの障害が発生することがあります。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義することによって，バックボーンが結合されることになり，この障害を回避できます。

図 17-16　バックボーン間の接続

(c) バックボーンの障害による分断に対する経路の予備

次の図では，バックボーンでネットワークの障害が発生し，ルータ 1 とルータ 2 の間の接続が切断された場合，バックボーンが分断されます。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを定義すると，これがバックボーンの分断に対する予備の経路（バックボーンでのルータ 1-ルータ 2 のコストと比較して，仮想リンクのコストが十分に小さい場合には，主な経路）となります。

図 17-17　バックボーン分断に対する予備経路

(d) 仮想リンクについての注意事項

仮想リンクを設定および運用するに当たって，次の注意事項に留意してください。

- 仮想リンクは，仮想リンクの両端のルータで共に設定する必要があります。通過エリア上の任意のインタフェースに IPv6 グローバルまたは IPv6 サイトローカルアドレスが定義されている必要があります。また，IPv6 グローバルまたは IPv6 サイトローカルアドレスを一つも広告していない隣接ルータとは仮想リンクは動作しません。
- 仮想リンクのコストは，通過エリアでの仮想リンクの両端のルータ間の経路コストになります。
- 通過エリアで，仮想リンクの両端のルータ間の経路がイコールコストマルチパスの場合，一般のトラフィックと仮想リンク上の経路情報トラフィックでは，経路が異なることがあります。
- 仮想リンク上の Hello パケットの送信間隔 (hellointerval) は，通過エリア上での仮想リンクの両端ルータ間の経路を構成する各ネットワーク上の，各インタフェースに設定してある Hello パケットの送信間隔のどれよりも長くする必要があります。この値をどれよりも短く設定した場合，通過エリア内の経路上のネットワークの障害にあたって，通過エリア内の代替経路への交替に基づいて仮想リンクが使用する経路が交替するよりも先に，仮想リンクが切断することがあります。
- 仮想リンク上の OSPFv3 パケットの再送間隔 (retransmitinterval) は，仮想リンクの両端ルータ間をパケットが往復するのに必要な時間よりも十分に長く設定する必要があります。ただし，あまり長過ぎる値を設定すると，混雑しているネットワーク上での仮想リンクの運用時に仮想リンク上での経路情報の交換に障害が発生することがあります。

17.5.4　ルータ間の接続の検出

OSPFv3 が動作しているルータは，ルータ間の接続性を検出するため，インタフェースごとに Hello パケットを送信します。Hello パケットを他ルータから受信することによって，ルータ間で OSPFv3 が動作していることを認識します。

(1) ルータ間接続条件

ブロードキャスト型とポイント - ポイント型とに関係なく，ルータ間を直接接続するネットワークのそれぞれについて，接続するルータのインタフェースの OSPFv3 の定義は，次に示す項目が一致している必要があります。これが一致していないルータ間では，OSPFv3 上は接続していないことになります。

(a) エリア ID

ルータ間の直接接続では，両ルータのインタフェースに定義したエリアが一致している必要があります。

(b) HelloInterval と RouterDeadInterval

OSPFv3 では，直接接続しているルータに，自ルータを検出させるために，Hello パケットを送信します。HelloInterval は Hello パケットの送信間隔，RouterDeadInterval は，あるルータからの Hello パケットを受信できないことを理由に，そのルータとの接続が切れたと判断するまでの時間です。検出と切断を適切に判断するためには，直接接続しているルータのインタフェースに定義した，この二つの値が一致している必要があります。

（c） エリアの定義

スタブエリアとスタブでないエリアとでは，エリアに通知される情報が異なります。このため，OSPFv3 が二つのルータを直接接続していると判断するには，インタフェースが所属しているエリアのスタブについての定義が一致している必要があります。

（d） インスタンス ID

OSPFv3 では，接続しているルータを複数のグループに分けるためにグループの識別子としてインスタンス ID を広告します。定義したインスタンス ID は，経路情報を交換するルータのインタフェースに定義したインスタンス ID と一致している必要があります。

（e） OSPFv3 を使用するインタフェースの設定についての注意事項

OSPFv3 では，インタフェースに定義してある送信時パケットの最大長 (MTU) と同じ長さのパケットを送信する場合があります。ここで，受信側のインタフェースに定義してある受信時パケットの最大長 (MRU：特に記述がなければ，MTU と同一) よりも長い場合，通常のトラフィックでは顕在化しないルータ間の相互通信不可能の問題が発生する場合があります。このため，OSPFv3 を使用する場合は，特にすべてのネットワークおよびネットワークに接続しているすべてのルータのインタフェースについて，MTU が他のすべてのインタフェースの MRU 以下に定義してあることの確認をお勧めします。

（2） ブロードキャスト型ネットワークと指定ルータ

ブロードキャスト型ネットワークでは，トポロジ上の頂点であるネットワークとネットワークに直接接続しているルータ間の接続情報を管理するために，指定ルータ (Designated Router) とバックアップ指定ルータを選択します。指定ルータの障害時には，ネットワークの接続情報の管理ルータを速やかに移行するために，バックアップ指定ルータが指定ルータになります。

指定ルータおよびバックアップ指定ルータの選択には，ルータのネットワークへのインタフェースに定義する priority(コンフィグレーションコマンド interface(ospf6 area モード) の priority サブコマンド) を使用します。指定ルータが存在しない場合，バックアップ指定ルータを指定ルータに選択します。指定ルータもバックアップ指定ルータも存在しない場合は最も priority の高いルータを指定ルータに選択します。指定ルータは存在するが，バックアップ指定ルータが存在しない場合，指定ルータを除いて最も priority の高いルータをバックアップ指定ルータに選択します。両ルータとも存在する場合，新しくより priority の高いルータが現れても，選択は変更しません。

あるルータのあるインタフェースの priority を 0 と定義すると，このルータはインタフェースが接続しているエリアについて，指定ルータにもバックアップ指定ルータにも選択されません。

ブロードキャスト型ネットワーク上に複数のルータがあり，このネットワークをトラフィックの転送に使用する場合は，どれかのルータのネットワークに接続しているインタフェースの priority を 1 以上にする必要があります。

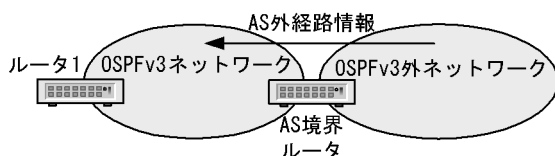
（a） 指定ルータについての注意事項

接続しているルータ数の多いネットワークでは，指定ルータの負荷は高くなります。このため，このようなネットワークに複数接続しているルータが存在する場合，このルータが，複数のネットワークの指定ルータにならないように，priority を設定することをお勧めします。

17.5.5 AS 外経路と AS 境界ルータ

OSPFv3 では，OSPFv3 を使用しているルータが AS 外の経路情報を認識している場合，この経路を OSPFv3 を使用してそのほかすべての OSPFv3 を使用しているルータに通知できます。OSPFv3 を使用

し，AS 外経路を OSPFv3 内に導入するルータを **AS 境界ルータ**と呼びます。本装置を AS 境界ルータとして使用するためには，エキスポート・フィルタのコンフィグレーション (コンフィグレーションコマンド export の配布先プロトコルに ospf6ase を指定) が必要となります。AS 外経路情報の導入の概念を次の図に示します。

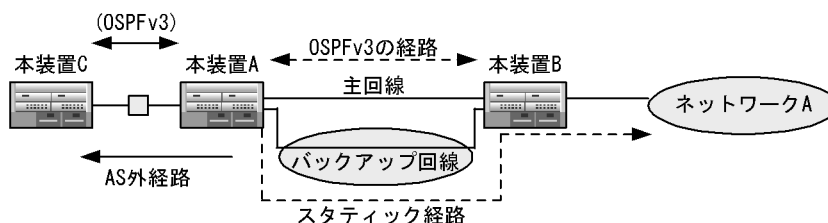
図 17-18　AS 外経路情報の導入の概念

(1) AS 外経路の広告

OSPFv3 へ AS 外経路を導入するとき，導入元の AS 境界ルータは，宛先までのメトリック，AS 外経路メトリックタイプ，フォワーディングアドレスとタグを付加して広告します。

- メトリック
  宛先までのメトリックとして，固定の値を指定します (コンフィグレーションコマンド defaults(ospf6 モード) の cost サブコマンド，コンフィグレーションコマンド route-filter または export コマンドの metric パラメータ)。また，RIPng のようにメトリックの情報を含んだ経路情報を OSPFv3 へ取り込む場合には，メトリック引き継ぎ指定 (コンフィグレーションコマンド defaults(ospf6 モード) の inherit-metric サブコマンド) によって，メトリックを引き継ぐことができます。
- AS 外経路メトリックタイプ
  OSPFv3 へ導入する AS 外経路には，Type 1 と Type 2 の 2 種類があります。Type 1 と Type 2 の経路では，経路の優先順位，およびメトリックを経路の選択に使用するときの計算方法が異なります。
- フォワーディングアドレス (転送先)
  本装置では設定しません。
- タグ
  付加情報としてタグを広告できます。

(2) AS 外経路の導入例

バックアップ回線を使用した構成での AS 外経路の導入例を次の図に示します。

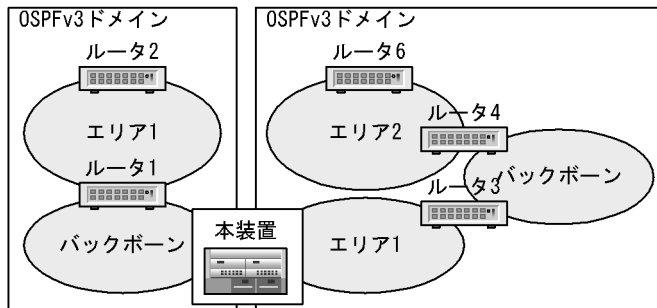
図 17-19　バックアップ回線を使用した構成での AS 外経路の導入例

OSPFv3 では，隣接するルータを検出するために，定期的にパケットを交換します。このため，バックアップ回線を OSPFv3 のトポロジの一部として使用した場合，この回線でパケットを継続して交換するため，バックアップ回線も常に運用状態になります。バックアップ回線上での通信が必要ではない場合にバックアップ回線を休止状態とするには，次のように設定します。

本装置 A では主回線で OSPFv3 を動作させ，バックアップ回線にネットワーク A へのスタティック経路

を定義します。デフォルトでは，OSPFv3 の AS 内経路のプリファレンス値はスタティック経路のプリファレンス値と比べ小さい（優先度が高い）ため，ネットワーク A への経路は OSPFv3 で学習した AS 内経路が選択されます。主回線障害時，本装置 A では該当する AS 内経路が削除されスタティック経路を再選択しますが，本装置 C ではネットワーク A への経路情報が存在しなくなります。本装置 A でのネットワーク A へのスタティック経路情報を AS 外経路として本装置 C に広告するためには本装置 A でエキスポート定義を設定する必要があります。こうすることによって，バックアップ回線上で Hello パケットを交換しないで主回線障害時にも OSPFv3 にネットワーク A への有用な経路情報を導入できます。

17.5.6 OSPFv3 マルチバックボーン機能

本装置では，1 台のルータ上で AS を複数の OSPFv3 ネットワークに分割し，OSPFv3 ネットワークごとに別個に経路の交換，計算，生成を行うことができます。この機能を **OSPFv3 マルチバックボーン**と呼びます。OSPFv3 マルチバックボーン機能の構成例を次の図に示します。以降，独立した各 OSPFv3 ネットワークのことを，**OSPFv3 ドメイン**と呼びます。OSPFv3 ドメインは，最大四つ定義できます。

図 17-20 OSPFv3 マルチバックボーン機能の構成例

1 台のルータが接続している複数の OSPFv3 ドメインは，それぞれ独立した OSPFv3 ネットワークとして動作します。このため，経路再配布についてのコンフィグレーションの定義がない場合には，一方の OSPFv3 ドメイン上の経路が他方の OSPFv3 ドメインへ配布されることはありません。すなわち，各ドメインは互いに異なるプロトコルとして動作します。経路再配布については「17.6　経路フィルタリング (RIPng/OSPFv3)」を参照してください。

(1) マルチバックボーン機能使用時の注意事項

(a) マルチバックボーン使用についての注意

ネットワークを複数の OSPFv3 ドメインに分割して運用した場合，ルーティングループの抑止やコストに基づいた経路選択などの OSPFv3 の特長が，OSPFv3 ドメイン間の経路の選択や配布によって失われます。新規ネットワーク構築時など，ネットワークを複数の OSPFv3 ドメインに分割して運用する必要がない場合には，単一の OSPFv3 ネットワークとして構築することをお勧めします。

(b) 複数ドメイン使用時のインタフェース定義についての注意

インタフェースを同時に複数の OSPFv3 ドメインに定義しないでください。本装置に接続している各インタフェースは，それぞれ一つのドメインの一つのエリアだけに所属できます。複数のドメインで OSPFv3 インタフェースとして定義した場合，対象のインタフェースは，どの OSPFv3 ドメインでも OSPFv3 インタフェースとして動作しなくなります。

(c) 装置アドレス使用についての注意

装置アドレスを複数の OSPFv3 ドメインに広告する必要がある場合には，OSPFv3 AS 外経路として広告してください。装置アドレスを OSPFv3 AS 外経路として広告するには，「17.6.2 エキスポート・フィルタ (RIPng/OSPFv3)」を参照してください。

17.5.7 経路選択の優先順位

本装置は，各プロトコルで学習した同一宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同一宛先への経路情報が各プロトコルでの生成によって複数存在する場合，それぞれの経路情報のプリファレンス値が比較され優先度の最も高い経路情報が有効となります。
OSPFv3 内における経路選択の優先順位を次の表に示します。

表 17-12 経路選択の優先順位

優先順位	選択項目	詳細
高	経路情報の種類	OSPFv3 の AS 内経路は，AS 外経路より優先します。
↑	学習元ドメイン	• 複数ドメインに経路が存在する場合，プリファレンス値が最小である経路を選択します。プリファレンス値が等しい場合，OSPFv3 ドメイン番号が最小の経路を選択します。
	経路の宛先タイプ	• AS 内経路：エリア内経路は，エリア間経路より優先します。 • AS 外経路：エリア内の AS 境界ルータが広告している経路が，別エリアの AS 境界ルータが広告している経路よりも優先します。
	AS 外経路タイプ	Type1 の AS 外経路は，Type 2 の AS 外経路より優先します。
	AS 外経路で経由するエリア	エリアボーダであるルータでは，宛先の AS 境界ルータが複数のエリアに接続している場合，AS 境界ルータまでのコスト値が最も小さいエリアを選択します。コスト値が等しい場合，エリア ID の最も大きいエリアを選択します。
	コスト	• AS 内経路：宛先までのコスト値が最も小さい経路を優先します。 • Type1 の AS 外経路：AS 外経路情報のメトリック値と AS 境界ルータまでのコスト値の合計が最も小さい経路を選択します。 • Type2 の AS 外経路：AS 外経路情報のメトリック値が最も小さい経路を選択します。メトリック値が等しい場合，AS 境界ルータまでのコスト値が最も小さい経路を選択します。
	ルータ ID	ネクストホップであるルータのルータ ID が最も小さい経路を選択します。
↓ 低	インタフェース ID	ネクストホップであるルータから，Hello パケットで最も小さいインタフェース ID を学習したインタフェースを選択します。

注 1
コンフィグレーションコマンド ospf6 の multipath サブコマンドを定義することによって，AS 内経路について，学習元ドメインと宛先タイプとコストが等しい経路を複数選択できます。AS 外経路についても同様に，学習元ドメインと AS 外経路タイプとコストが等しい経路を複数選択できます。

注 2
選択項目の優先順位は変更できません。

17.5.8 グレースフル・リスタート

(1) 概要

グレースフル・リスタートは，装置の BCU が系切替したり，運用コマンドなどによりルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機

能です。グレースフル・リスタート機能一般については，「12.8　グレースフル・リスタートの概要」を参照してください。

OSPFv3 では，グレースフル・リスタートによって OSPFv3 の再起動を行う装置のことをリスタートルータといいます。リスタートルータにあるグレースフル・リスタートをする機能をリスタート機能といいます。また，グレースフル・リスタートを補助する隣接装置をヘルパールータといいます。ヘルパールータにあるグレースフル・リスタートを補助する機能をヘルパー機能といいます。

SB-7800S では，リスタート機能とヘルパー機能をサポートしています。

SB-5400S では，ヘルパー機能だけをサポートしています。

OSPFv3 のコンフィグレーションでは，ドメインごとにリスタート機能とヘルパー機能の動作可否を指定できます。

以下に，OSPFv3 でグレースフル・リスタート機能を使用するときの構成上の条件を示します。以下の条件を満たさない場合，グレースフル・リスタートに失敗したり，グレースフル・リスタートが終了するまで通信できない経路ができたりすることがあります。

- グレースフル・リスタートするルータに，リスタート機能を設定してください。本装置でリスタート機能を設定する場合，コンフィグレーションコマンド options で graceful-restart パラメータを設定し，コンフィグレーションコマンド ospf6 の graceful-restart サブコマンドで mode restart または mode both を設定してください。
- グレースフル・リスタートするルータの隣接ルータすべてに，ヘルパー機能を設定してください。本装置でヘルパー機能を設定する場合，コンフィグレーションコマンド ospf6 の graceful-restart サブコマンドで mode helper または mode both を設定してください。

(2) リスタート機能【SB-7800S】

(a) リスタート機能の動作契機

以下に，本装置で OSPFv3 のリスタート機能が動作する契機を示します。

- BCU が系切替したとき。
- ルーティングプログラムが再起動したとき。

(b) グレースフル・リスタートの手順

次の図および次の表に OSPFv3 のグレースフル・リスタート手順を示します。

図 17-21 OSPFv3 グレースフル・リスタート手順

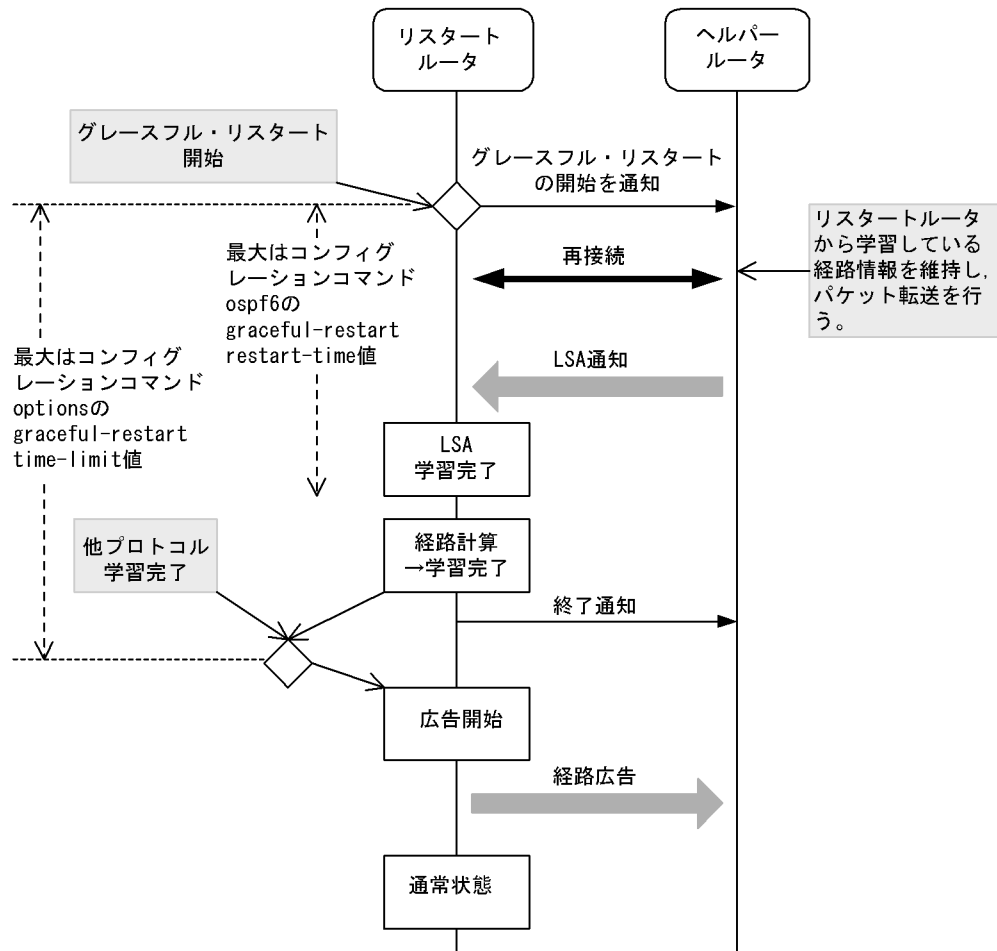



表 17-13 OSPFv3 グレースフル・リスタート手順

項番	項目	契機	処理内容
1	グレースフル・リスタートの開始	BCU が系切替したとき。	グレースフル・リスタートを開始します。通常の接続手順と同様に，各インタフェースで OSPFv3 情報のパケット交換を行います。
		ルーティングプログラムが再起動したとき。	
2	経路計算	ドメイン内の全 OSPFv3 インタフェースについて再接続完了し，隣接ルータからすべての LSA を学習したとき。	ドメインごとに経路計算を行い，ルーティングテーブルを更新します。 複数のドメインが存在する場合，経路計算は接続の終わったドメインから随時行います。経路計算が全ドメインで終了したとき，OSPFv3 の経路学習が完了します。
		1 インタフェースでもグレースフル・リスタートに失敗したとき。	その時点での同一ドメイン内の各インタフェースの接続状態に基づいて，経路計算を行います。
3	広告開始	OSPFv3 の経路学習が完了し，かつ他のルーティングプロトコルの経路学習が完了したとき。	AS 外経路の広告を開始します。広告完了後，通常の OSPFv3 動作に戻ります。
		OSPFv3 のグレースフル・リスタートに失敗したとき。	

(c) グレースフル・リスタートが失敗するケース

以下に OSPFv3 のグレースフル・リスタートが失敗するケースを示します。

- グレースフル・リスタートの開始をヘルパールータへ通知してからコンフィグレーションコマンド ospf6 の graceful-restart restart-time の時間が経過しても LSA 学習を完了できなかった場合。
- 再接続を行っているインタフェースがダウンした場合。
- OSPFv3 ドメイン上で LSA が変更された場合。
- OSPFv3 ドメイン上の別のルータがグレースフル・リスタートした場合。
- グレースフル・リスタートを開始してから経路保持時間 (コンフィグレーションコマンド options の graceful-restart time-limit の時間) が経過しても全プロトコルの経路学習が完了しなかった場合。
- コンフィグレーションコマンド ospf6 の graceful-restart mode を変更し，リスタートルータ機能を削除した場合。
- コンフィグレーションコマンド options を変更し，グレースフル・リスタート機能を削除した場合。

(d) 注意事項

1. リスタートルータとして，グレースフル・リスタートを開始しても，一部のヘルパールータがヘルパー動作を開始しない場合や，途中で止めた場合，同一ドメイン内の全インタフェースでグレースフル・リスタートを止めます。
2. OSPFv3 のリスタート時間 (コンフィグレーションコマンド ospf6 の graceful-restart restart-time の時間) を，系切替所要時間 + LSA 学習時間を超えるように設定してください。これは，OSPFv3 が LSA を学習するためには，系切替が完了して IPv6 インタフェースの Up/Down を確認できるようになっている必要があるためです。グレースフル・リスタート開始後，リスタート時間が経過した時点で LSA の学習が終わってない場合，OSPFv3 のグレースフル・リスタートに失敗します。
   系切替所要時間については，「12.8　グレースフル・リスタートの概要 表 12-30　系切替所要時間の目安値」を参照してください。
3. 本装置の系切替時ルーティングエントリ保持時間を，OSPFv3 のリスタート時間よりも長く設定してください。OSPFv3 のリスタート時間よりもルーティングエントリ保持時間のほうが短い場合，経路学習前に系切替前ルーティングエントリが削除されることがあります。
4. BGP4+ のルーティングピアがグレースフル・リスタートを使用している場合，ルーティングピアのリスタート時間を OSPFv3 のリスタート時間よりも長く設定してください。
   ルーティングピアのリスタート時間のほうが短い場合，OSPFv3 が経路学習を完了する前にルーティングピアを接続することができず，ルーティングピアのグレースフル・リスタートに失敗することがあります。

(3) ヘルパー機能

本装置は，ヘルパールータとして動作している場合，グレースフル・リスタートを行っている間，リスタートルータを経由する経路を維持します。

(a) ヘルパー機能の動作条件

ヘルパー機能が動作する条件を以下に示します。

- 既に同一ドメイン内で別のリスタートルータのヘルパーとなっていないこと。同一ドメイン内で，複数ルータのグレースフル・リスタートに対して同時にヘルパールータとして動作できません。ただし，リスタートルータが 1 台しかない場合，そのリスタートルータと接続しているインタフェースすべてでヘルパールータとして動作を行います。
- 自ルータがリスタートルータとして，グレースフル・リスタートを実行していないこと。**【SB-7800S】**
- リスタートルータに送信した OSPFv3 の Update パケットに対する Ack 待ちの状態でないこと。

(b) ヘルパー機能が失敗するケース

ヘルパールータとしての動作は，隣接が確立するまで，または，リスタートルータから終了の通知を受信するまで継続します。

しかし，以下のイベントが発生した場合，リスタートルータが維持している経路と不整合が発生する可能性があるため，ヘルパー機能を中断し，経路を再計算します。

- 隣接ルータから新しい LSA(定期更新を除く) を学習し，リスタートルータへ広告した場合。
- OSPFv3 インタフェースがダウンした場合。
- リスタートルータ以外のルータとの隣接関係の切断または確立によって LSA を更新した場合。
- OSPFv3 の同一ドメイン内で，複数のルータが同時に再起動した場合。
- コンフィグレーションコマンド ospf6 の graceful-restart mode を変更し，ヘルパー機能を削除した場合。

(c) 注意事項

1. 本装置の OSPFv3 隣接ルータで OSPFv3 リスタート機能を使用する場合，本装置に OSPFv3 ヘルパー機能を設定してください。

17.5.9　スタブルータ

(1) 概要

隣接ルータとの接続が完了していなかったり，安定していなかったりすると，ネットワーク全体のルーティングが不安定になることがあります。ルータの起動時・再起動時やネットワークにルータを追加するときに，このような状況がおこることがあります。OSPFv3 ではこのような状況下，周辺の装置でルーティングにできるだけ使用されないように，経路情報を通知することができます。OSPFv3 では，このような通知を行っているルータを，スタブルータと呼びます。この機能によって，装置の状態が不安定であっても，ネットワークのルーティングが不安定になることを防ぐことができます。

(2) スタブルータ動作

スタブルータは，接続する OSPFv3 インタフェースのコスト値を最大値（65535）にして広告します。このため，スタブルータを経由する OSPFv3 経路は優先されなくなります。

ただし，隣接ルータの存在しないインタフェース（スタブネットワーク）の経路については，コンフィグレーションで指定したコスト値を広告します。スタブネットワークや AS 外経路はスタブルータの経路が優先されることがあります。

周辺装置では，コスト比較により，スタブルータを経由しない代替経路を優先します。また，スタブルータ自身の装置アドレスを使用して，telnet による管理や BGP4+ による経路交換ができます。

OSPFv3 のコンフィグレーションでは，ドメインごとにスタブルータ機能を動作させるかどうかを指定できます。さらに，動作条件として，スタブルータとして常時動作させるか，または起動後に動作させるかを選択できます。

(3) 常時動作する場合

常時，コストを最大値にします。スタブルータのコンフィグレーションを削除するまで，動作し続けます。

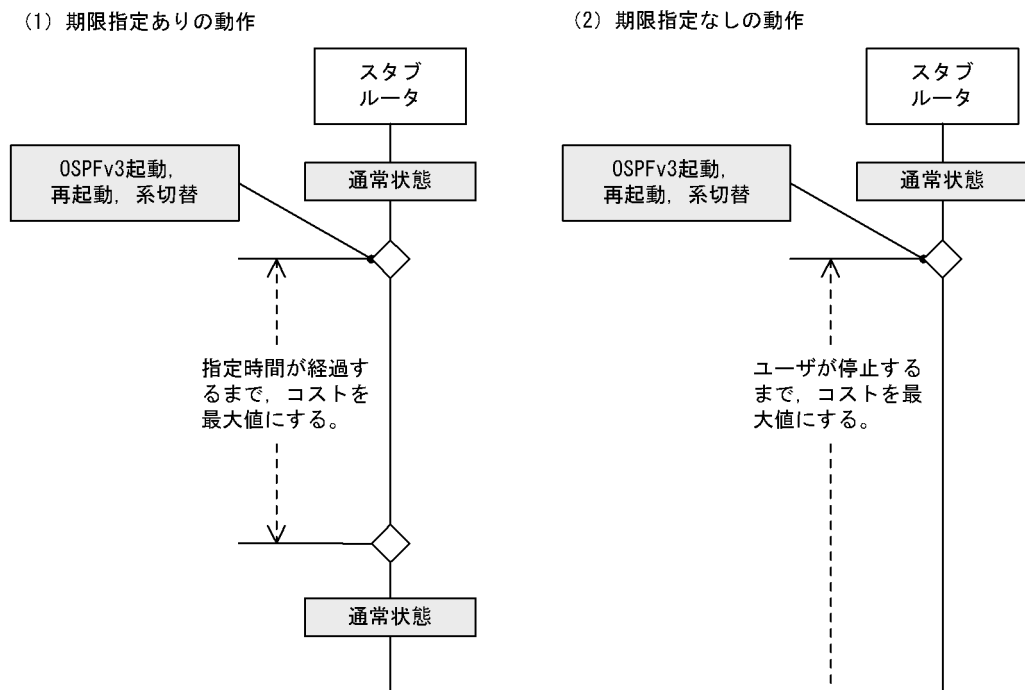
(4) 起動後にスタブルータとして動作する場合

次に示す契機でコストを最大値にします。コンフィグレーションで指定した期限が経過するまで，継続します。

- BCU の系切替後（グレースフル・リスタート成功時を除く）
- ルーティングプログラムの再起動後（グレースフル・リスタート成功時を除く）
- グレースフル・リスタートが発生し，本装置がリスタートルータとしての経路学習に失敗した後
- 装置起動

コンフィグレーションを変更し，起動後にスタブルータとして動作することを指定した場合，次回の起動・再起動・系切替から適用されます。

動作中に運用コマンド clear ipv6 ospf stub-router を実行するか，コンフィグレーションを削除することで停止できます。スタブルータの動作を次の図に示します。

図 17-22　スタブルータの動作

（5） 注意事項

1. グレースフル・リスタートのヘルパールータとして動作しているとき，スタブルータのコンフィグレーションを変更しないでください。定義を変更すると，スタブルータが動作を開始したり，終了したりして，ヘルパー動作に失敗することがあります。
2. スタブルータとして常時動作する定義になっているとき，起動後に動作するように変更すると，すぐにスタブルータを終了します。
3. 仮想リンクの通過エリアでのコストが 65535 よりも大きい場合，仮想ネーバはその仮想リンクを到達不能とみなします。このため，スタブルータを通過する仮想リンクは，使用できません。

17.5.10　高速経路切替機能

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報（第 1 優先経路と呼ぶ）と，第 1 優先経路の次に優先される経路（第 2 優先経路と呼ぶ）をあらかじめルーティングテーブルに登録しておき，インタフェースダウンによって第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディング・テーブルに登録することで，通信停止時間の短縮を図る機能です。

OSPFv3 単独で第 1 優先経路と第 2 優先経路の両方をルーティングテーブルに登録することはできませんが，スタティック経路など OSPFv3 以外のプロトコルで生成した同一宛先の経路を組み合わせることによって，この機能を適用することが可能です（「表 18-7　高速経路切替を適用する経路の組み合わせ」を参照してください）。

高速経路切替機能の詳細については「18.2.5　高速経路切替機能」を参照してください。

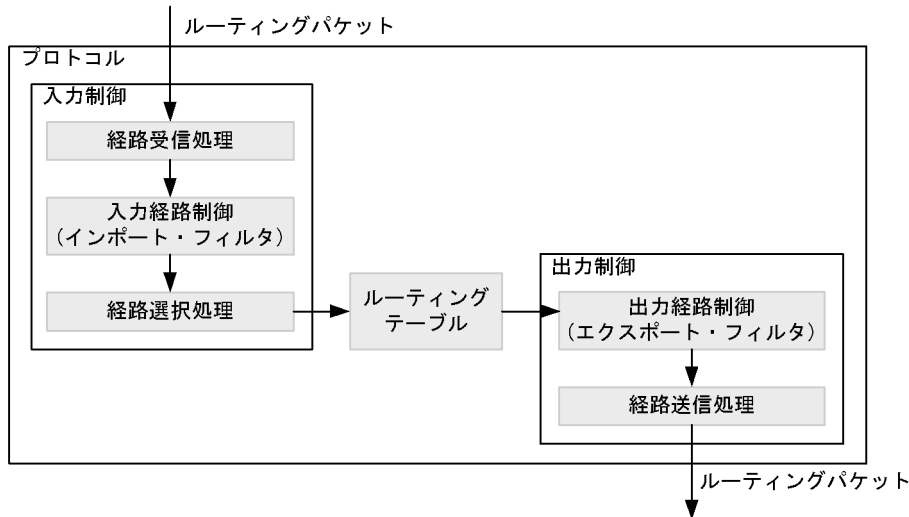
17.5.11　OSPFv3 使用時の注意事項

OSPFv3 を使用したネットワークを構成する場合には，次の制限事項に留意してください。

- OSPFv3 の制限事項
  本装置は，RFC2740(OSPF for IPv6) に準拠しています。しかし，ソフトウェアの機能制限によって，次に示す機能はサポートしていません。
  - Point-to-Multipoint インタフェース
  - AS 外経路のフォワーディングアドレスに基づく経路選択
  - 非ブロードキャスト (NBMA) ネットワーク

17.6 経路フィルタリング (RIPng/OSPFv3)

経路フィルタリングには，入力経路を制御するインポート・フィルタと出力経路を制御するエキスポート・フィルタがあります。インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。エキスポート・フィルタは同一ルーティングプロトコル，またはルータ上で同時に動作している異なるプロトコルで学習した経路を広告するかどうかを制御します。フィルタリングの概念を次の図に示します。

図 17-23　フィルタリングの概念

17.6.1 インポート・フィルタ (RIPng/OSPFv3)

インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。インポート・フィルタを指定していない場合は，すべての経路情報を取り込みます。

また，取り込まれた経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，そのプロトコルのデフォルトのプリファレンス値となります。インポート・フィルタのフィルタリング条件を次の表に示します。

表 17-14　インポート・フィルタのフィルタリング条件

プロトコル	フィルタリング条件
RIPng	• 受信インタフェース • 送信元ゲートウェイ • 経路情報の宛先ネットワーク
OSPF6ASE	• OSPFv3 ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク

17.6.2 エキスポート・フィルタ (RIPng/OSPFv3)

エキスポート機能はルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。学習元プロトコルで学習した経路情報を配布先プロトコルを使用しほかのシステム（ルータ）

に広告します。

(1) フィルタリング条件

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件 (送出先) と学習元プロトコルのフィルタリング条件 (送出経路情報) によって，特定の宛先に特定の経路情報を送出できます。また，配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値となります。

指定できるフィルタリング条件を配布先プロトコルと学習元プロトコルに分け「表 17-15　配布先プロトコルのフィルタリング条件」および「表 17-16　学習元プロトコルのフィルタリング条件」に示します。

表 17-15　配布先プロトコルのフィルタリング条件

配布先プロトコル	フィルタリング条件 (送出先)	付加情報
RIPng	• 送信元インタフェース	• メトリック値
OSPF6ASE	• OSPFv3 ドメイン番号 ただし，学習元が同じ OSPFv3 ドメインの OSPF6，OSPF6ASE の場合は制御できません。	• メトリック値 • AS 外経路タイプ • タグ値

表 17-16　学習元プロトコルのフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIPng	• 受信インタフェース • 送信元ゲートウェイ • 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIPng で学習された経路情報
OSPF6	• OSPFv3 ドメイン番号 • 経路情報の宛先ネットワーク	OSPFv3 で学習された経路情報
OSPF6ASE	• OSPFv3 ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPFv3 の AS 外経路情報
DIRECT	• インタフェース • 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 送出元インタフェース • 経路情報の宛先ネットワーク	スタティックの経路情報
DEFAULT【**OP-BGP**】	• 経路情報の宛先ネットワーク	BGP4+ の DEFAULT 経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

(2) 再配布する経路情報のメトリック値

フィルタリング条件には再配布する経路情報のメトリック値，またはメトリック値に加算する値を指定できます。RIPng で再配布する経路情報のメトリック値を「表 17-17　再配布する経路情報のメトリック値 (RIPng)」に，OSPFv3 で再配布する経路情報のメトリック値を「表 17-18　再配布する経路情報のメトリック値 (OSPF6ASE)【OP-OSPF(SB-5400S)】」に示します。

また，フィルタリング条件でオフセット指定 (+ 指定) した場合に，RIPng で再配布する経路情報のメトリック値を「表 17-19　オフセット指定した場合に再配布する経路情報のメトリック値 (RIPng)」に，OSPFv3 で再配布する経路情報のメトリック値を「表 17-20　オフセット指定した場合に再配布する経路

情報のメトリック値 (OSPF6ASE)【OP-OSPF(SB-5400S)】」に示します。

表 17-17　再配布する経路情報のメトリック値 (RIPng)

metric 指定	学習元プロトコル	配布先プロトコル (RIPng)
あり	RIPng	経路情報のメトリック値を引き継ぎます。
	その他	エキスポート・フィルタで指定したメトリック値を使用します。
なし	RIPng	経路情報のメトリック値を引き継ぎます。
	直結経路	直結経路 (ブロードキャスト型回線) の場合，1 で広告します。直結経路 (ポイント - ポイント型回線の自装置側インタフェース) の場合，1 で広告します。直結経路 (ポイント - ポイント型回線の相手装置側インタフェース) の場合，2 で広告します。
	集約経路	集約経路の場合，1 で広告します。
	OSPF6，OSPF6ASE，BGP4+，IS-IS	コンフィグレーションコマンド ripng の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値または MED 属性値を引き継ぎます。ただし，値が 1~15 以外の場合は，RIPng として広告しません。そのほかの場合，デフォルト・メトリック値を使用します。
	スタティック経路，デフォルト経路	デフォルト・メトリック値を使用します。

表 17-18　再配布する経路情報のメトリック値 (OSPF6ASE)【**OP-OSPF(SB-5400S)**】

metric 指定	学習元プロトコル	メトリック値
あり	全プロトコル共通	エキスポート・フィルタで指定したメトリック値を使用します。
なし	OSPF6	コンフィグレーションコマンド defaults(ospf6 モード) の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値を引き継ぎ，経路の種類が type 1 になります。上記以外でコンフィグレーションコマンド ospf6 の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。
	OSPF6ASE (Type 1)	コンフィグレーションコマンド defaults(ospf6 モード) の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値と経路の種類 (type 1) も引き継ぎます。さらにタグ値も引き継ぎます。上記以外でコンフィグレーションコマンド ospf6 の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。
	OSPF6ASE (Type 2)	コンフィグレーションコマンド defaults(ospf6 モード) の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値に 1 を加えた値と経路の種類 (type 2) も引き継ぎます。さらにタグ値も引き継ぎます。上記以外でコンフィグレーションコマンド ospf6 の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。
	RIPng，直結経路，集約経路，BGP4+，スタティック経路，デフォルト経路，IS-IS	コンフィグレーションコマンド defaults(ospf6 モード) の inherit-metric サブコマンドを指定した場合，経路情報のメトリック値を引き継ぎます。ただし，経路情報にメトリック値，または MED 属性値がない場合は，0 を使用します。 また，BGP4+ 経路の MED 値が 16777215(10 進数) 以上の場合，OSPF6ASE として広告しません。経路の種類はデフォルト (コンフィグレーションコマンド ospf6 で指定のない場合は type 2) になります。上記以外でコンフィグレーションコマンド ospf6 の cost サブコマンド (パラメータ) を指定した場合，その指定値を使用します。そのほかの場合，デフォルト・メトリック値を使用します。

注　学習元プロトコルの OSPF6，OSPF6ASE は配布先と異なるドメインに所属する OSPF6，OSPF6ASE を示します。同一ドメインへの経路情報は再配布しません。

また，メトリック値以外に配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値となります。

表 17-19　オフセット指定した場合に再配布する経路情報のメトリック値 (RIPng)

学習元プロトコル	メトリック値
RIPng，直結経路，集約経路，スタティック経路，デフォルト経路	「表 17-17　再配布する経路情報のメトリック値 (RIPng)」に示している再配布時に使用する経路情報のメトリック値に，オフセット値を加算した値を使用します。
OSPF6，OSPF6ASE，BGP4+，IS-IS	「表 17-17　再配布する経路情報のメトリック値 (RIPng)」に示している再配布時に使用する経路情報のメトリック値に，オフセット値を加算した値を使用します。ただし，コンフィグレーションコマンド ripng の inherit-metric サブコマンド指定によって，引き継いだメトリック値，または MED 属性値が 0 の場合は，0 を基準にオフセット値を加算した値を使用します。

注　オフセット値の加算結果が 16 以上になった場合，経路情報は再配布しません。

表 17-20　オフセット指定した場合に再配布する経路情報のメトリック値 (OSPF6ASE)【OP-OSPF(SB-5400S)】

学習元プロトコル	メトリック値
OSPF6，OSPF6ASE	ドメイン間で経路情報を再配布する場合は，「表 17-18　再配布する経路情報のメトリック値 (OSPF6ASE)【OP-OSPF(SB-5400S)】」に示している再配布時に使用する経路情報のメトリック値に，オフセット値を加算した値を使用します。同一ドメインへの経路情報の再配布は行わないため，オフセット値の加算も行いません。
RIPng，BGP4+，直結経路，集約経路，スタティック経路，デフォルト経路，IS-IS	「表 17-18　再配布する経路情報のメトリック値 (OSPF6ASE)【OP-OSPF(SB-5400S)】」に示している再配布時に使用する経路情報のメトリック値に，オフセット値を加算した値を使用します。

注　オフセット値の加算結果が 16777215 以上になった場合，経路情報は再配布しません。

17.7 経路集約 (RIPng/OSPFv3)

経路集約は一つまたは複数の経路情報から該当する経路情報を包含するようなネットワークマスクの，より短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含するような一つの経路情報を生成して，隣接ルータなどに集約経路を通知することによって，ネットワーク上の経路情報の数を少なくする方法です。例えば，3ffe:501:811:ff01::/64 の経路情報や 3ffe:501:811:ff02::/64 の経路情報を学習した場合に 3ffe:501:811:ff::/56 の集約された経路情報を生成するというようなものです。

経路集約の指定はコンフィグレーションコマンド aggregate(経路集約) で明示的に指定する必要があります。経路情報を特定するための集約元経路情報のフィルタリング条件を次の表に示します。

表 17-21　集約元経路情報のフィルタリング条件

集約元プロトコル	フィルタリング条件 (集約元経路情報)	備考
RIPng	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIPng で学習された経路情報
OSPF6	• 経路情報の宛先ネットワーク	OSPFv3 の AS 内経路情報
OSPF6ASE	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPFv3 の AS 外経路情報
DIRECT	• 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 経路情報の宛先ネットワーク	スタティックの経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

また，集約元経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，集約経路のデフォルトのプリファレンス値 (130) が使用されます。なお，集約元の経路情報が学習されていない場合には集約経路情報は生成されません。

(1) 集約元経路の広告抑止

集約元経路の広告抑止の詳細は，「12.7　経路集約 (RIP/OSPF) （1）集約元経路の広告抑止」を参照してください。

(2) 集約経路の転送方法

集約経路によるパケット転送方法の詳細は，「12.7　経路集約 (RIP/OSPF) （2）集約経路の転送方法」を参照してください。

17.8　グレースフル・リスタートの概要 (RIPng/OSPFv3)

IPv6 でのグレースフル・リスタートの動作は IPv4 と同様です。詳細は「12.8　グレースフル・リスタートの概要」を参照してください。

18 BGP4+【OP-BGP】

この章では BGP4+ の仕様や使用する上での注意点を中心に説明します。

18.1 BGP4+ 概説

BGP4+(Multiprotocol Extensions for Border Gateway Protocol 4) は，インターネットのバックボーンで使用されているルーティングプロトコル BGP4 を，IPv4 以外のプロトコルにも使用できるように拡張したものです。インターネット上で使用されているすべての経路情報を扱えます。経路情報は今後のネットワークの拡大にも対応し，200000 経路まで拡張できます。

BGP4+(IPv6) と BGP4(IPv4) の機能差分を次の表に示します。

表 18-1　BGP4+(IPv6) と BGP4(IPv4) の機能差分

機能	BGP4+(IPv6)	BGP4(IPv4)
EBGP，IBGP ピアリング，経路配信	○	○
経路フィルタ，BGP 属性変更	○	○
コミュニティ	○	○
ルート・リフレクション	○	○
コンフィデレーション	○	○
サポート機能のネゴシエーション	○	○
ルート・リフレッシュ	○	○
マルチパス	○	○
ポリシーグループ※1	○	○
ルート・フラップ・ダンピング	○	○
BGP4 MIB	×	○
TCP MD5 認証	○	○
グレースフル・リスタート	○※2	○※2

（凡例）　○：取り扱う　×：取り扱わない

注※1　外部ピア同士，または内部ピア同士のグルーピング

注※2　SB-5400S ではレシーブルータの機能だけサポートします。

18.1.1 経路情報

本装置が取り扱う経路情報（ルーティング対象とするアドレスの種類）を次の表に示します。

表 18-2　経路情報

経路情報の種類		説明
通常の経路	デフォルト経路	すべてのネットワーク宛ての経路。 （プレフィックス：::/0）
	グローバルネットワーク経路	特定のネットワーク宛てのグローバル経路およびそれを集約した経路。
	グローバルホスト経路	特定のホスト宛ての経路。（ネットワークマスクが 128 ビットの経路）
ルーティング 対象外の経路	リンクローカル経路	（プレフィックス：fe80::% 回線名 /64）
	マルチキャストアドレス	（プレフィックス：ff00::/8）
	IPv4 予約アドレス	（プレフィックス：::/8）

18.1.2　BGP4+ の適用範囲

BGP4+ で取り扱う経路情報および機能を次の表に示します。

表 18-3　BGP4+ で取り扱う経路情報および機能

経路情報		BGP4+
経路情報	デフォルト経路	○
	グローバルネットワーク経路	○
	グローバルホスト経路	○
	マルチパス	○
経路選択		AS パス属性
ルーティングループ抑止		○
認証機能		○

（凡例）　○：取り扱う

18.1.3　ネットワーク設計の考え方

本装置を使用しネットワークを設計する上でいくつかの注意事項がありますので,「17.2　ネットワーク設計の考え方」も併せて参照してください。

18.2 経路制御 (BGP4+)

18.2.1 スタティックルーティング

スタティックルーティングはコンフィグレーションで設定した経路情報 (スタティック経路) に従ってパケットを中継する機能です。スタティックルーティングについては「17.3.1 スタティックルーティング」を参照してください。

18.2.2 ダイナミックルーティング (BGP4+)

本装置では RIPng，OSPFv3，BGP4+ をサポートしています。RIPng については「17.4 RIPng」に，OSPFv3 については「17.5 OSPFv3【OP-OSPF(SB-5400S)】」に，BGP4+ については「18 BGP4+【OP-BGP】」に示します。

18.2.3 スタティックルーティングとダイナミックルーティング (BGP4+) の同時動作

(1) プリファレンス値

複数のルーティング種別が同時動作するとき，それぞれは独立した経路選択手順に従い，ある宛先アドレスへの経路情報から一つの最良の経路を選択します。その結果，ルータ内ではある宛先アドレスへの経路情報が複数存在することになります。このような場合，それぞれの経路情報のプリファレンス値が比較されて優先度の高い経路情報が有効になります。

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコル (例えば BGP4+) ごとに生成する経路情報のデフォルトのプリファレンス (優先度) 値をコンフィグレーションで設定できます。なお，プリファレンスは値の小さい方の優先度が高くなります。各プロトコルのプリファレンスのデフォルト値を次の表に示します。

表 18-4 プリファレンスのデフォルト値

経路	デフォルトプリファレンス値
直結経路	0(固定値)
OSPFv3 の AS 内経路	10
IS-IS の内部経路	15
BGP4+ のデフォルト経路	20
スタティック経路	60
RIPng 経路	100
集約経路	130
OSPFv3 の AS 外経路	150
IS-IS の外部経路	160
BGP4+ 経路	170

(2) エキスポート機能

本装置では，学習した経路情報を BGP4+ で広告したい場合や，特定の経路情報の広告をフィルタリングしたい場合には**エキスポート機能**によって実現できます。

エキスポート機能では，コンフィグレーションで学習元プロトコルと配布先プロトコル (BGP4+) を指定することによって，特定ルーティングプロトコルで学習した経路を BGP4+ で広告できます。

(a) BGP4+ で学習した経路の広告

BGP4+ 経路のエキスポート設定をしていない場合，同一ルーティングプロトコルで学習した経路情報であっても広告されません。ある AS から学習した BGP4+ 経路を他の AS に広告するためにはエキスポートの定義が必要です。

エキスポートの設定によって広告される経路情報は BGP4+ で選択された最良の経路です。

(b) BGP4+ 以外で学習した経路の広告

複数のルーティングプロトコルが同時動作するとき，BGP4+ 以外のルーティングプロトコルで学習した経路情報はエキスポートの定義をすることで広告されます。

エキスポートの設定によって広告される経路情報はプリファレンス値によって選択された最も優先度の高い経路です。

(c) 同一宛先経路の広告

BGP4+ で学習した経路情報と他のルーティングプロトコルで学習した経路情報が同一宛先である場合，エキスポートの設定により広告される経路情報が異なります。同一宛先経路の広告条件を次の表に示します。

表 18-5　同一宛先経路の広告条件

学習元プロトコルのエキスポート許可指定		広告条件
BGP4+	BGP4+ 以外※	
未指定	未指定	広告しません。
	指定	• 指定した学習元プロトコルで学習した経路情報のうち，プリファレンス値によって選択された最も優先度の高い経路情報を広告します。 • 学習した経路情報の優先度が低い場合はエキスポートを設定しても広告しません。
指定	未指定	• BGP4+ で学習した経路情報のうち，最良の経路を広告します。 • BGP4+ 以外で学習した経路情報が BGP4+ の経路情報より優先度の高い場合でも，BGP4+ 経路を広告します。
	指定	• 指定した学習元プロトコルで学習した経路情報のうち，プリファレンス値によって選択された最も優先度の高い経路情報を広告します。 • BGP4+ 以外で学習した経路情報の方が優先度が高い場合，その経路情報がエキスポート対象でなければ最良の BGP4+ 経路を広告します。

注※　RIPng，OSPF6，OSPF6ASE，DIRECT，STATIC，DEFAULT，AGGREGATE のどれかを示します。

18.2.4　経路削除保留機能

経路削除保留機能は，ルーティングプロトコルが無効にした経路を，ルーティングテーブルから一定時間削除しないようにすることで，新しく代替経路が生成されるまでの間，既存経路によってフォワーディングを維持する機能です。

経路削除保留機能については，「13.2.4　経路削除保留機能」を参照してください。

18.2.5 高速経路切替機能

(1) 概要

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報 (第 1 優先経路と呼ぶ) と，第 1 優先経路の次に優先される経路 (第 2 優先経路と呼ぶ) をあらかじめルーティングテーブルに登録しておき，インタフェースダウンなどによって，第 1 優先経路が使用不可能になったとき，素早く第 2 優先経路をフォワーディングテーブルに登録することで，通信停止時間の短縮を図る機能です。

高速経路切替のサポート範囲を次の表に示します。

表 18-6　高速経路切替のサポート範囲

切替契機	切替内容
インタフェースダウン	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わない IGP 経路の変更による BGP4+ 経路の NextHop 変更	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わないピア切断による BGP4+ 経路の NextHop 変更	第 2 優先経路への切り替え
	マルチパス経路の縮退

高速経路切替を適用する経路の組み合わせを次の表に示します。

表 18-7　高速経路切替を適用する経路の組み合わせ

項目		第 1 優先経路※3※4								
		BGP4+	OSPFv3	RIPng	IS-IS	スタティック (gateway 指定)※1	スタティック (remote-gateway 指定)※1	スタティック (interface 指定)※1※2	集約経路	直結経路
第 2 優先経路※3※4	BGP4+	○	○	○	○	○	○	○	×	×
	OSPFv3	○	-	○	○	○	○	○	×	×
	RIPng	○	○	○	○	○	○	○	×	×
	IS-IS	○	○	○	-	○	○	○	×	×
	スタティック (gateway 指定)※1	○	○	○	○	○	○	○	×	×
	スタティック (remote-gateway 指定)※1	○	○	○	○	○	○	○	×	×
	スタティック (interface 指定)※1※2	○	○	○	○	○	○	○	×	×
	集約経路	×	×	×	×	×	×	×	-	×
	直結経路	×	×	×	×	×	×	×	×	-

(凡例)　○：適用する　　×：適用しない　　-：この組み合わせは発生しない

注※ 1

コンフィグレーションコマンド static の reject サブコマンドまたは noinstall サブコマンドを指定した場合は高速経路切替を適用しない。

注※ 2

Null インタフェース，local-address または broadcast 型インタフェースを指定した場合は高速経路切替を適用しない。

注※ 3

IPv6 over IPv4 トンネル，6to4 トンネルを送出インタフェースとする経路については，高速経路切替を適用しない。

注※ 4

第 1 優先経路または第 2 優先経路をルーティングテーブルに追加後，本経路に高速経路切替機能が適用されるまで，1 万経路当たり約 3 秒の時間を要します。

その間，経路切替契機が発生しても，高速経路切替が適用されない場合があります。

(2) BGP4+ プロトコルによる適用例 (第 2 優先経路への切り替え)

次の図の様に，BGP4+ プロトコルが複数のピアから学習した同一宛先の経路情報で高速経路切替を行うには，コンフィグレーションコマンド options の fast-reroute パラメータと，コンフィグレーションコマンド bgp4+ の fast-reroute サブコマンドで gen-secondary-route パラメータを設定し，第 2 優先経路を生成する必要があります。この場合，「18.3.2 経路選択アルゴリズム」で示す優先順位が，最も高い経路が第 1 優先経路に，2 番目に高い経路が第 2 優先経路に選択されます。なお，第 1 優先経路と第 2 優先経路のプリファレンス値が同じ値でない場合には，第 2 優先経路は生成しません。

図 18-1 BGP4+ プロトコルによる高速経路切替機能の適用例 (第 2 優先経路への切り替え)

この図で本装置 A は，ネットワーク B 宛の経路情報を学習した本装置 B および本装置 D とピアを形成し，ネットワーク B 宛の経路情報を本装置 B および本装置 D のそれぞれから学習しています。本装置 B から

学習した経路情報は本装置 D から学習した経路情報よりも優先度が高いとします。また，本装置 B は，ネットワーク A 宛の経路情報を学習した本装置 A および本装置 C とピアを形成し，ネットワーク A 宛の経路情報を本装置 A および本装置 C のそれぞれから学習しています。本装置 A から学習した経路情報は本装置 C から学習した経路情報よりも優先度が高いとします。

この状態で第 2 優先経路を生成するように設定した場合，本装置 A および本装置 B から学習した経路を第 1 優先経路，本装置 C および本装置 D から学習した経路を第 2 優先経路とし，第 1 優先経路をフォワーディングテーブルに登録します。これによって本装置 A ではネットワーク B 宛の経路は本装置 B にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 A にルーティングします (図の (a) のケース)。

このとき，本装置 A と本装置 B との間で障害が発生し，第 1 優先経路が使用不可能になると，即座に第 2 優先経路をフォワーディングテーブルに登録し，本装置 A ではネットワーク B 宛の経路は本装置 D にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 C にルーティングします (図の (b) のケース)。

このように，本装置 A と本装置 B でインタフェース障害を検出して即座に第 2 優先経路に切り替えることで通信停止時間を短縮できます。

(3)　BGP4 プロトコルによる適用例 (マルチパス経路の縮退)

コンフィグレーションコマンド options の fast-reroute パラメータが設定されている場合，マルチパス経路の縮退が高速化されます。

図 18-2　BGP4+ プロトコルによる高速経路切替機能の適用例 (マルチパス経路の縮退)

(a) 経路切り替え前

(b) 経路切り替え後

この図で本装置 A は，ネットワーク B 宛の経路情報を学習した本装置 B および本装置 D とピアを形成し，

ネットワーク B 宛の経路情報を本装置 B および本装置 D のそれぞれから学習しています。本装置 B から学習した経路情報と本装置 D から学習した経路情報の優先度は同一とします。また，本装置 B は，ネットワーク A 宛の経路情報を学習した本装置 A および本装置 C とピアを形成し，ネットワーク A 宛の経路情報を本装置 A および本装置 C のそれぞれから学習しています。本装置 A から学習した経路情報と本装置 C から学習した経路情報の優先度は同一とします。

この状態で BGP マルチパスが設定されている場合，本装置 A は本装置 B から学習した経路と本装置 D から学習した経路の間でマルチパスを形成しフォワーディングテーブルに登録します。また，本装置 B は本装置 A から学習した経路と本装置 C から学習した経路の間でマルチパスを形成しフォワーディングテーブルに登録します。これによって本装置 A ではネットワーク B 宛の経路は本装置 B または本装置 D にルーティングし，本装置 B ではネットワーク A 宛の経路は本装置 A または本装置 C にルーティングします (図の (a) のケース)。

このとき，本装置 A と本装置 B との間で障害が発生し，マルチパスの一方が使用不可能になると，使用不可能となったパスを即座にフォワーディングテーブルから削除し，本装置 A はネットワーク B 宛の経路はすべて本装置 D にルーティングし，本装置 B はネットワーク A 宛の経路はすべて本装置 C にルーティングします (図の (b) のケース)。

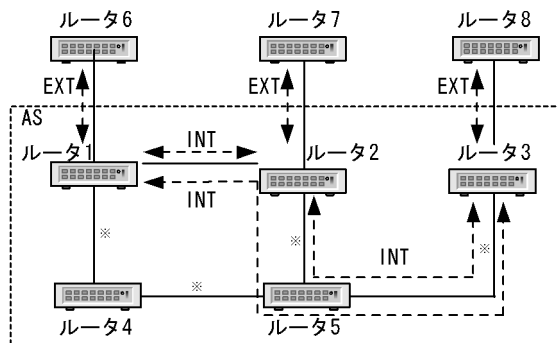
18.3　BGP4+

18.3.1　BGP4+ の基礎概念

BGP4+ は AS 間のルーティングプロトコルであり，扱う経路情報は，宛先ネットワークへの AS パス情報（パケットが宛先のネットワークに到達するまでに通過する AS の列）で構成されます。BGP4+ が動作するルータを **BGP4+ スピーカ**といいます。この BGP4+ スピーカはほかの BGP4+ スピーカと経路情報を交換するためにピアを形成します。

(1)　ピアの種類

本装置で使用されるピアには外部ピアおよび内部ピアの 2 種類があります。内部ピアはインターナルピアおよびルーティングピアがあります。ネットワーク構成に合わせてピアを使用してください。内部ピアと外部ピアの例を次の図に示します。

図 18-3　内部ピアと外部ピアの例

- **外部ピア (エキスターナルピア)**
  異なる AS に属する BGP4+ スピーカ間に形成するピアです。ピアリングに使用する IPv6 アドレスは直接接続されたインタフェースのリンクローカルまたはグローバルインタフェースアドレスを使用します。
  「図 18-3　内部ピアと外部ピアの例」のルータ 1- ルータ 6 間，ルータ 2- ルータ 7 間，ルータ 3- ルータ 8 間に形成されるピアです。
- **内部ピア**
  同じ AS に属する BGP4+ スピーカ間に形成するピアです。BGP4+ はピア間のコネクションを確立するために TCP(ポート 179) を使用します。内部ピアは AS 内の各 BGP4+ スピーカ間でフルメッシュに形成されなければなりません。これは，内部ピアで受信した経路情報はほかの内部ピアに通知されないためです。
  - **インターナルピア**
    同じ AS 内に属し，物理的に直接接続された BGP4+ スピーカ間に形成するピアです。ピアリングに使用する自側 IPv6 アドレスには直接接続されたインタフェースのリンクローカル以外のインタフェースアドレスを使用します。装置アドレスを使用する場合はルーティングピアとなります。
    「図 18-3　内部ピアと外部ピアの例」のルータ 1- ルータ 2 間に形成されるピアです。
  - **ルーティングピア**

同じ AS 内に属し，物理的に直接接続されない BGP4+ スピーカ間に形成するピアです。ピアリングに使用する自側 IPv6 アドレスはそのルータの装置アドレス，またはルータ内のインタフェースのリンクローカル以外のインタフェースアドレスのどちらかになります。
「図 18-3　内部ピアと外部ピアの例」のルータ 1- ルータ 3 間，ルータ 2- ルータ 3 間に形成されるピアです。

注意事項

コンフィデレーション構成時は，これら三つのピア種別に加え，メンバー AS 間ピア (サブ AS 間ピア) が追加されます。メンバー AS 間ピアの説明は「18.3.6　コンフィデレーション」を参照してください。

(2) 装置アドレス

本装置では装置に対して IPv6 アドレスを割り当てることができます。これを装置アドレスと呼びます。この装置アドレスを内部ピアの IPv6 アドレスとして使用すると，特定の物理インタフェースの状態に依存した内部ピア (TCP コネクション) への影響を排除できます。

例えば，「図 18-3　内部ピアと外部ピアの例」でルータ 1- ルータ 2 間の内部ピアにインタフェースの IPv6 アドレスを使用すると，ルータ 1- ルータ 2 間に障害が発生してインタフェースが使用できない場合には，ルータ 1- ルータ 2 間の内部ピアは確立できません。しかし，内部ピアの IPv6 アドレスとして装置アドレスを使用すると，ルータ 1- ルータ 2 間のインタフェースが使用できない場合でもルータ 4，ルータ 5 経由で内部ピアを確立できます。

装置アドレス使用上の注意事項

装置アドレスを使用する場合，そのアドレスへの経路情報をスタティックまたは IGP(RIPng, OSPFv3) でお互いに学習していなければなりません。なお，本装置は，装置アドレスを直結経路情報として扱います。

ルーティングピアで非 BGP4+ スピーカを経由する場合の注意事項

ルーティングピアで非 BGP4+ スピーカを経由して経路情報を通知する (例えば，ルータ 2 からルータ 3 に通知する) 場合，非 BGP4+ スピーカでは IGP 経由でその経路情報を学習していなければなりません。これは該当する経路情報の通知によって通知先 BGP4+ スピーカから入ってくる該当する宛先への IPv6 パケットが，該当する経路を学習していない非 BGP4+ スピーカのルータで廃棄されるのを防ぐためです。例えば，ルータ 3 からルータ 5 に入ってくる IPv6 パケットがルータ 5 で廃棄されるのを防ぐためです。

18.3.2　経路選択アルゴリズム

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同じ宛先への経路情報が各プロトコルで生成されて複数存在する場合は，それぞれの経路情報のプリファレンス値が比較され優先度の最も高い経路情報が有効になります。

BGP4+ では，自プロトコルを使用して学習した同じ宛先への複数の経路情報か優先順位に従って一つの最良の経路を選択します。経路選択の優先順位を次の表に示します。その後，同じ宛先への経路情報が各プロトコル (RIPng，OSPFv3，スタティック) で経路を選択することによって複数存在する場合は，それぞれの経路情報のプリファレンス値が比較され，優先度の最も高い経路情報をルーティングテーブルに設定します。

表 18-8　経路選択の優先順位

優先順位	内容
高	LOCAL_PREF 属性の値が最も大きい経路を選択します。
↑	AS_PATH 属性の AS 数が最も短い経路を選択します。
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。
	外部ピアで学習した経路，内部ピアで学習した経路の順で選択します。
	ネクストホップが最も近い (ネクストホップ解決時に使用した IGP 経路のメトリック値が最も小さい) 経路を選択します。
↓	相手 BGP 識別子 (ルータ ID) が最も小さい経路を選択します。
低	比較する経路が BGP4+ マルチパスの関係にある場合に，学習元ピアのアドレスが若い経路を選択します。

経路選択に関連する経路情報に含まれる BGP 属性 (LOCAL_PREF 属性，AS_PATH 属性，ORIGIN 属性，MED 属性，MP_REACH_NLRI 属性のネクストホップ情報) の概念を次に説明します。

経路選択上の注意事項

1. AS_PATH 属性上のパスタイプ AS_SET は全体で一つの AS としてカウントします。
2. コンフィグレーションコマンド bgp4+ の compare-aspath サブコマンドに no オプションを指定することによって，AS パス長による経路選択を無効化できます。
3. MED 値による経路選択は，同一隣接 AS から学習した重複経路に対してだけ有効です。なお，コンフィグレーションコマンド bgp4+ の compare-med サブコマンドに all-as を指定することによって，異なる隣接 AS から学習した重複経路に対しても有効となります。

(1) LOCAL_PREF 属性

LOCAL_PREF 属性は，同じ AS 内のルータ間で通知される属性です。同じ宛先ネットワークに対し複数の経路がある場合，LOCAL_PREF 属性は該当する宛先ネットワークに対する優先経路を示します。より大きい LOCAL_PREF 属性値を持つ経路が優先されます。本装置で使用できる LOCAL_PREF 属性の使用範囲とデフォルト値を次の表に示します。

表 18-9　LOCAL_PREF 属性の使用範囲とデフォルト値

項目	内容	備考
使用範囲	0 ～ 65535	-
デフォルト値	100	default-localpref サブコマンドによって変更できます。

(凡例)　- : 該当しない

LOCAL_PREF 属性による経路選択の例については，「13.3.2　経路選択アルゴリズム」を参照してください。

(a) LOCAL_PREF 属性のフィルタ単位での変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の localpref サブコマンド (パラメータ) を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の LOCAL_PREF 属性を変更できます。

(2) AS_PATH 属性

AS_PATH 属性は，経路情報の宛先ネットワークに到達するまでに通過する AS 番号のリストです。経路情報がそのほかの AS に通知されるとき，その経路情報の AS_PATH 属性に自 AS 番号を追加します。AS_PATH 属性による経路選択の例については，「13.3.2 経路選択アルゴリズム」を参照してください。

(a) 追加 AS パス数の変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の ascount サブコマンド (パラメータ) を組み合わせることによって，複数の自 AS 番号を AS_PATH 属性に追加できます。これはある宛先ネットワークへの複数の経路がある場合に特定の経路を選択するのに有効です。

(3) ORIGIN 属性

ORIGIN 属性は，経路情報の生成元を示します。ORIGIN 属性を次の表に示します。経路選択では，同一宛先への複数の経路が存在する場合，IGP，EGP，Incomplete の順で選択します。

表 18-10 ORIGIN 属性

ORIGIN 属性	内容
IGP	該当する経路が AS 内部で生成されたことを示します。
EGP	該当する経路が EGP 経由で学習されたことを示します。
Incomplete	該当する経路が上記以外の方法で学習されたことを示します。

(a) ORIGIN 属性の変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の origin サブコマンド (パラメータ) を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の ORIGIN 属性を変更できます。

(4) MED 属性

MED 属性は，同一の隣接 AS から学習した，ある宛先への複数の BGP4+ 経路の優先度を決める属性です。より小さい MED 属性値を持つ経路情報が優先されます。MED 属性による経路選択の例については，「13.3.2 経路選択アルゴリズム (4) MED 属性」を参照してください。

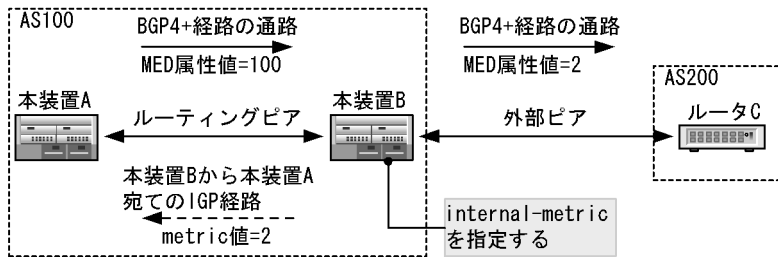
(a) MED 属性による経路選択の変更

コンフィグレーションコマンド bgp4+ の compare-med サブコマンドに all-as を指定することによって，異なる隣接 AS から学習した BGP4+ 経路間の優先度選択に使用できます。

(b) MED 属性の変更

本装置ではインポート・フィルタやエキスポート・フィルタとコンフィグレーションコマンド attribute-list/route-filter の med サブコマンド (パラメータ) を組み合わせることによって，自装置内に取り込む経路情報や通知する経路情報の MED 属性を変更できます。

また，med サブコマンド (パラメータ) に internal-metric を指定した場合，NextHop 解決に使用している IGP 経路のメトリック値を，通知する BGP4+ 経路の MED 属性値にすることができます。internal-metric の使用例を次の図に示します。

図 18-4　internal-metric の使用例

この図では本装置 A，本装置 B の間でルーティングピアを形成しているものとします。MED 属性値 =100 で本装置 A から通知された BGP4+ の経路情報を本装置 B がルータ C に通知するとき，本装置 B から本装置 A までの IGP 経路のメトリック値 =2 を MED 属性値に設定したい場合，本装置 B のエキスポート・フィルタで med サブコマンド (パラメータ) に internal-metric を指定します。

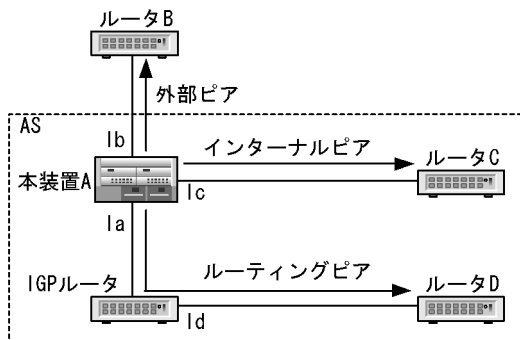
(5) MP_REACH_NLRI 属性のネクストホップ情報

BGP4+ では BGP4+ ピアから受信した NextHop 属性の値を無視します。その代わりに MP_REACH_NLRI 属性のネクストホップ情報を経路のネクストホップとして採用します。

BGP4+ では相手 BGP4+ スピーカに経路情報を通知する場合，MP_REACH_NLRI 属性のネクストホップ情報としてピアリングに使用した自側 IPv6 グローバルアドレスでピアリングした場合だけ，ピアリングに使用した自側インタフェースのリンクローカルアドレス (外部ピアの場合だけ) を設定します。

(a) ネクストホップ情報の設定例

通知する経路情報のネクストホップ例を次の図に示します。この例は本装置 A でのネクストホップ情報の設定例です。

図 18-5　通知する経路情報のネクストホップ例

- **外部ピアを形成するルータ B への経路情報**
  MP_REACH_NLRI 属性のネクストホップには，本装置 A とルータ B 間のインタフェースの，本装置 A 側のグローバルおよびリンクローカルアドレス Ib が割り当てられます。ルータ B が実際のネクストホップとしてどちらを採用するかは，本装置 A は関知しません。
- **直接接続された外部ピアを形成するルータ B からの経路情報**
  MP_REACH_NLRI 属性のネクストホップにグローバルアドレスとリンクローカルアドレスとのどちらか一方だけが含まれていた場合は，そのアドレスをネクストホップとして使用します。両方のアドレスが含まれていた場合は，リンクローカルアドレスをネクストホップとして使用します。
- **内部ピア (インターナルピア) を形成するルータ C への経路情報**
  MP_REACH_NLRI 属性のネクストホップには，本装置 A とルータ C 間のインタフェースの本装置 A

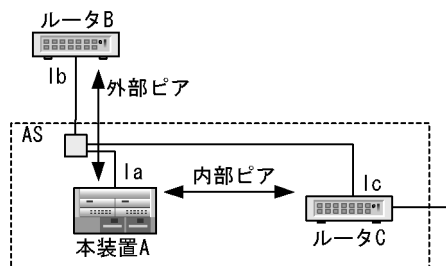
側グローバルアドレス (Ic) が使用されます。

- **内部ピア (ルーティングピア) を形成するルータ D への経路情報**
  MP_REACH_NLRI 属性のネクストホップには，本装置 A と IGP ルータ間のインタフェースの本装置 A 側グローバルアドレス Ia が使用されます。
  なお，ピアリングアドレスに「18.3.1　BGP4+ の基礎概念」で説明した装置アドレスを使用している場合には，装置アドレスが MP_REACH_NLRI 属性のネクストホップに設定されます。
- **内部ピア (インターナルピア，ルーティングピア) からの経路情報**
  MP_REACH_NLRI 属性のネクストホップにリンクローカルアドレスが含まれていても，グローバルアドレスをネクストホップとして使用します。MP_REACH_NLRI 属性のネクストホップにリンクローカルアドレスだけが含まれている場合はネクストホップが不正であると判断して，その経路情報を無視します。

(b)　ネクストホップ情報を書き換えない場合

ブロードキャスト型インタフェースで接続されたピア間で経路情報を通知する場合，通常通知する経路情報のネクストホップ情報は書き換えません。ただし，外部ピアから受信した経路情報を内部ピアへ通知する場合に，外部ピアから受信したリンクローカルネクストホップ情報を廃棄します。

ブロードキャスト型インタフェース接続でのネクストホップ情報の設定例を次の図に示します。

図 18-6　ブロードキャスト型インタフェース接続でのネクストホップ情報の設定例

外部ピアを形成するルータ B から通知された経路情報を内部ピアを形成するルータ C に通知する場合，通知するネクストホップ情報はルータ B から通知されたグローバルネクストホップ Ib となります。

ルータ C から通知された経路情報をルータ B に通知する場合，通知する経路情報のネクストホップはルータ C から通知されたグローバルネクストホップ Ic になります。つまり，通知する経路情報のネクストホップが通知するインタフェースと同一のネットワーク上に存在する場合，グローバルネクストホップ情報は書き換えません。ルータ B でリンクローカルネクストホップが必要な場合は，本装置 A で nexthopself オプションを指定してください。このオプションがあると，ルータ A がルータ B に広告する経路のネクストホップがルータ B へのインタフェースのグローバルアドレス Ia，リンクローカルアドレス Ia になります。

(c)　ネクストホップの解決

ルーティングピアから BGP4+ 経路情報を学習した場合，MP_REACH_NLRI 属性のネクストホップ情報で示されたアドレスへ到達するためのパスを，IGP 経路，スタティック経路，および直結経路によって解決します。BGP4+ 経路のネクストホップへ到達可能な経路の中から，宛先のマスク長が最も長い経路を選択し，当該経路のパスを BGP4+ 経路のパスとして使用します。また，bgp4+ コンフィグレーションコマンドの resolve-nexthop オプションで all を指定すると，上記の経路に加えて，BGP4+ 経路をネクストホップの解決に使用します。

なお，ネクストホップを解決した経路がスタティック経路で，かつ，noinstall オプションの指定がある場

合，当該 BGP4+ 経路を抑止します。この機能は次のような場合に利用できます。

- 宛先不明の中継トラフィックを廃棄するため，null インタフェース向けのデフォルト経路を設定してあるルータで，当該デフォルト経路によって BGP4+ 経路のネクストホップが解決されてしまうことを防ぐために，ネクストホップ宛のスタティック経路を定義し，noinstall オプションを指定します。

18.3.3 サポート機能のネゴシエーション

サポート機能のネゴシエーション (Capability Negotiation) は，BGP コネクション確立時の OPEN メッセージに Capability 情報を付加することによって，ピア間で使用できる機能をネゴシエーションする機能です。お互いに広告した Capability 情報で一致する (お互いにサポートする) 機能を該当するピアで使用できます。

本装置では，「IPv6-Unicast 経路の送受信」の Capability を常に設定し，Capability 関連パラメータをコンフィグレーションで定義した場合，OPEN メッセージにその Capability 情報を付加します。Capability 情報を持たない OPEN メッセージで確立した BGP コネクションは，「IPv6-Unicast 経路の送受信」だけを行います。ネゴシエーションできる機能を次の表に示します。

表 18-11　ネゴシエーションできる機能

機能名称	サブコマンド	内容
IPv6-Unicast 経路の送受信	ipv6-uni ※	IPv6-Unicast 経路を該当するピア間で送受信します。
ルート・リフレッシュ	refresh	ルート・リフレッシュ機能を使用します。
ルート・リフレッシュ (Capability Code 128)	refresh-128	Capability Code に 128 を使用する BGP4+ ピアと，ルート・リフレッシュ機能を使用します。
グルースフル・リスタート	graceful-restart	グレースフル・リスタート機能を使用します。

注※　IPv6-Unicast 経路の送受信 (ipv6-uni) サブコマンドは，コンフィグレーションの設定があるかどうかに関係なく，OPEN メッセージに Capability 情報を付加します。

18.3.4 ルート・リフレクション

BGP4+(IPv6) のルート・リフレクションの基本動作は BGP4(IPv4) でのルート・リフレクションと同様です。詳細は，「13.3.5　ルート・リフレクション」を参照してください。

18.3.5 コミュニティ

BGP4+(IPv6) のコミュニティの基本動作は BGP4(IPv4) でのコミュニティと同様です。詳細は，「13.3.3　コミュニティ」を参照してください。

18.3.6 コンフィデレーション

BGP4+(IPv6) のコンフィデレーションの基本動作は BGP4(IPv4) でのコンフィデレーションと同様です。詳細は，「13.3.6　コンフィデレーション」を参照してください。

18.3.7 ルート・リフレッシュ

ルート・リフレッシュ機能は，差分 UPDATE(変化が発生した経路だけを広告) を基本とする BGP4+ で，すでに広告された経路を強制的に再広告させる機能です。

ルート・リフレッシュ機能には，自装置側より経路を再広告する機能と BGP4+ ピアである相手装置側より経路を再広告させる機能があります。また，自装置から再広告するまたは相手装置から再広告させるための経路種別を選択できます。この機能は，clear ipv6 bgp コマンドの実行によって実行されます。

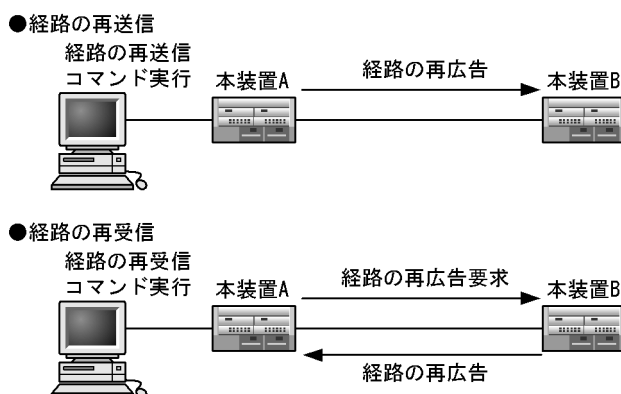
ルート・リフレッシュ機能を「表 18-12　ルート・リフレッシュ機能」に，ルート・リフレッシュ機能の動作概念を「図 18-7　ルート・リフレッシュ機能の動作概念図」に示します。

表 18-12　ルート・リフレッシュ機能

機能	経路種別	再広告方向
IPv6-Unicast 経路の再送信	IPv6 ユニキャスト経路	自装置側よりピアリングされた相手装置に経路を再広告します。
IPv6-Unicast 経路の再受信		ピアリングされた相手装置側より自装置に経路を再広告させます。

図 18-7　ルート・リフレッシュ機能の動作概念図

●経路の再送信

●経路の再受信

ルート・リフレッシュ使用時の注意事項

相手装置側からの経路の再送信は，ピアリングされた両ルータがルート・リフレッシュ機能をサポートしている必要があります。ルート・リフレッシュ機能を使用するかどうかは，BGP4+ ピア確立時にルート・リフレッシュ機能を使用することをお互いのルータ間でネゴシエーションすることによって決定します。このネゴシエーションによって，両ルータがルート・リフレッシュ機能をサポートしている場合だけ，相手装置側からの経路の再広告機能 (IPv6-Unicast 経路の再受信) を使用できます。本装置では，コンフィグレーションコマンド bgp4+ の refresh サブコマンドを指定することによって，ルート・リフレッシュ機能の使用を指定します。

また，本装置のルート・リフレッシュ機能は RFC2918 に準拠しています。ルート・リフレッシュ機能をサポートするそのほかの装置によっては，ここで説明したネゴシエーションで使用するルート・リフレッシュ用のネゴシエーション・コード値 (2) をベンダ固有のコード (128 ～ 255) でサポートしている装置もあります。本装置と他装置間でルート・リフレッシュ機能を使用するときは注意してください。

18.3.8　BGP4+ マルチパス

BGP4+(IPv6) でのマルチパスの基本動作は BGP(IPv4) でのマルチパスと同様です。詳細は，「13.3.7 BGP4 マルチパス」を参照してください。

IGP 経路のマルチパス化に伴う BGP4+ マルチパスの注意事項

本装置でマルチパス化を行える IGP 経路は，スタティック経路および OSPFv3 経路です。スタ

ティック経路のマルチパス化の概念は「17.3.1　スタティックルーティング」を，OSPFv3 経路のマルチパス化の概念は「17.5.2　経路選択アルゴリズム　(2) イコールコストマルチパス」を参照してください。

18.3.9　ルート・フラップ・ダンピング

BGP4+(IPv6) でのルート・フラップ・ダンピングの基本動作は BGP4(IPv4) でのルート・フラップ・ダンピングと同様です。詳細は，「13.3.4　ルート・フラップ・ダンピング」を参照してください。

18.3.10　TCP MD5 認証

BGP4+(IPv6) での TCP MD5 認証の基本動作は BGP4(IPv4) での TCP MD5 認証と同様です。詳細は，「13.3.10　TCP MD5 認証」を参照してください。

18.3.11　グレースフル・リスタート

BGP4+(IPv6) でのグレースフル・リスタートの基本動作は BGP4(IPv4) でのグレースフル・リスタートと同様です。詳細は「13.3.11　グレースフル・リスタート」を参照してください。

18.3.12　BGP4+ 経路の安定化機能

BGP4+(IPv6) での経路の安定化機能の基本動作は BGP4(IPv4) での経路の安定化機能と同様です。詳細は，「13.3.12　BGP4 経路の安定化機能」を参照してください。

18.3.13　BGP4+ 広告用経路生成

BGP4+(IPv6) での広告用経路生成の基本動作は BGP4(IPv4) での広告用経路生成と同様です。詳細は，「13.3.13　BGP4 広告用経路生成」を参照してください。

18.3.14　BGP4+ 学習経路数制限

BGP4+(IPv6) での学習経路数制限の基本動作は BGP4(IPv4) での学習経路数制限と同様です。詳細は「13.3.14　BGP4 学習経路数制限」を参照してください。

18.3.15　BGP4+ 使用時の注意事項

BGP4+ を使用したネットワークを構成する場合には次の制限事項に留意してください。

(1) BGP4+ の制限事項

本装置は RFC1771(BGP バージョン 4 仕様)，RFC2796(ルート・リフレクション仕様)，RFC1965(コンフィデレーション仕様)，RFC2842(サポート機能の広告仕様)，RFC2858(BGP4 マルチプロトコル拡張仕様)，RFC2918(ルート・リフレッシュ仕様)，RFC2545(RFC2858 の IPv6 適用方法の仕様)，RFC1997(コミュニティ仕様)に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 18-13 RFC との差分

RFC 番号	RFC		本装置
RFC1771	メッセージヘッダ形式	メッセージタイプが OPEN メッセージで認証を持つ場合，Marker の値は認証メカニズムで規定される計算で予測できます。	本装置では認証機能はサポートしていません。
	パス属性：NEXT_HOP	BGP スピーカが，同一 AS 内の BGP スピーカへ経路を広告するとき，広告するスピーカは，その経路についての NEXT_HOP 属性を修正すべきではありません。	BGP4+ では対象外です (NEXT_HOP 属性はダミーパラメータ)。
	パス属性：ATOMIC_AGGREGATE	BGP スピーカで，そのピアの一つから重複経路のセットが与えられ，より個別な (specific) 経路を選択しないで，より個別でない経路を選択する場合，ローカルシステムは，そのほかの BGP スピーカへ経路を伝えるとき，経路に ATOMIC_AGGREGATE 属性を付加すべきです。	本装置ではピアの一つから重複経路を受信し個別でない経路だけをインストールし，それをそのほかの BGP スピーカへ伝えるとき，経路に ATOMIC_AGGREGATE 属性を付加しません。
	コネクション衝突の発見	OPEN メッセージを受信したとき，ローカルシステムは OpenConfirm 状態にあるすべてのコネクションを検査する必要があります。また，プロトコル以外の手段によってピアの BGP 識別子を確認できれば，OpenSent 状態のコネクションも検査します。	OPEN メッセージを受信したとき，OpenSent 状態または Connect 状態のすべてのコネクションを検査します。
	バージョンネゴシエーション	BGP スピーカは，それぞれがサポートする最高のバージョンから始め，BGP コネクションのオープンを複数回試みることで，プロトコルのバージョンを取り決められます。	本装置は BGP4+(バージョン 4) だけサポートします。
	BGP FSM：IDLE 状態	エラーのために Idle 状態へ遷移したピアについて，続く Start までの間の時間は (Start イベントが自動的に生成されるなら)，指数的に増大するべきです。その最初のタイマ値は 60 秒です。時間はリトライごとに 2 倍にされるべきです。	本装置では Idle 状態から start までの間の最初のタイマは 16 〜 36 秒になります。
	BGP FSM：Active 状態	トランスポート・プロトコル・コネクションが成功した場合，ローカルシステムは ConnectRetry タイマをクリアし，初期設定を完了し，そのピアへ OPEN メッセージを送信し，その Hold タイマをセットし，状態を OpenSent へ変えます。Hold タイマの値は 4 分が提案されています。	本装置では Hold タイマはデフォルトで 180 秒 (3 分)，コンフィグレーションで指定されている場合はコンフィグレーションの値を使用します。
	経路広告の頻度	MinRouteAdvertisementInterval は，単一の BGP スピーカからの特定の宛先への経路広告の間隔の最小時間を決めます。このレート制限処理は，宛先ごとにされます。しかし，MinRouteAdvertisementInterval の値は，BGP ピアごとに設定されます。	本装置では MinRouteAdvertisementInterval はサポートしていません。
		MinASOriginationInterval は，広告する BGP スピーカ自身の AS 中の変化を報告するための連続した UPDATE メッセージ広告の間に経過しなければならない最小時間を決めます。	本装置では MinASOriginationInterval はサポートしていません。
	ジッタ	ある BGP スピーカによる BGP メッセージの配布がピークを含む可能性を最小にするために，MinASOriginationInterval，Keepalive，MinRouteAdvertisementInterval に関係したタイマにジッタを適用すべきです。	本装置ではジッタを適用していません。

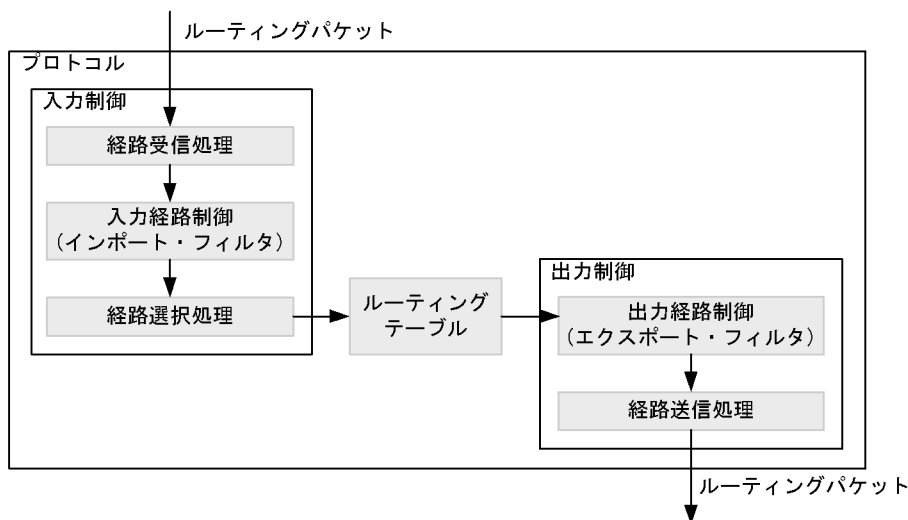
RFC 番号	RFC		本装置
	BGP タイマ	ConnectRetry タイマの提案されている値は 120 秒です。	本装置では ConnectRetry 回数により変化する可変値（16 〜 148 秒）になります。
		Hold Time の提案されている値は 90 秒です。	デフォルトの Hold Time は 180 秒です。コンフィグレーションに Hold Time が設定されている場合は，その値を使用します。
		KeepAlive タイマの提案されている値は 30 秒です。	本装置では Hold Time の 1/3 になります。
		BGP の実装は，これらのタイマがコンフィグレーションで定義可能でなければなりません。	本装置では Hold Time だけがコンフィグレーションで定義できます。
RFC2545	通知するネクストホップと通知先のピアとが同じネットワーク上にある場合に限り，リンクローカルネクストホップも通知します。		本装置では外部ピアが直結ネットワークで接続されている場合だけ RFC と同じ処理を行います。
	トランスポート・プロトコル	BGP4+ セッションに使用する TCP コネクションは IPv4 または IPv6 です。	本装置では IPv6 TCP による IPv6 経路情報通知だけサポートします。
	ピアリングアドレス種別	BGP4+ ピアリングに IPv4 または IPv6 アドレスを使用します。	本装置では IPv6 アドレスだけサポートします。インターナルピアおよびルーティングピアでは IPv6 リンクローカルアドレスでの BGP4+ 接続はサポートしていません。
RFC2858	MP_REACH_NLRI 属性	MP_REACH_NLRI 属性は経路，経路のネクストホップ，および SNPA(SubNetwork Points of Attachment) を通知するために使用します。	本装置では SubNetwork Points of Attachment はサポートしていません。
		内部 BGP ピア広告時は NEXT_HOP 属性 (BGP4+ では MP_REACH_NLRI 属性の Network Address of Next Hop フィールドに対応）を書き換えてはなりません (RFC1771)。	同一 AS 内の BGP スピーカへ経路を広告するとき MP_REACH_NLRI 属性の Network Address of Next Hop フィールドにその BGP スピーカとのピアリングに使用している自側の IPv6 アドレスを設定します。
	マルチプロトコル拡張 Capability	BGP Capability 広告によって BGP スピーカがどのアドレスファミリをサポートするかを通知します。	本装置では IPv6 ユニキャストアドレスだけサポートします。
RFC1965	メンバー AS 間ピアに経路情報を広告する場合，AS_PATH 属性にタイプ AS_CONFED_SEQUENCE で自メンバー AS 番号を追加します。		本装置では AS_PATH 属性にタイプ AS_CONFED_SET で自メンバー AS 番号を追加します。

(2)　直接接続されたインタフェース上でピアリングする場合の注意事項

直接接続されたインタフェース上の BGP スピーカ間で，本装置がインターナルピアまたはエキスターナルピアを使用し，かつ同一インタフェース上で本装置が OSPFv3 仮想リンクの通過エリアとなる構成の場合，ピアとコネクションが確立しません。この場合，コンフィグレーションコマンドの bgp4+ の multihop サブコマンドを設定することによって，コネクションが確立します。

18.4 経路フィルタリング (BGP4+)

経路フィルタリングには，入力経路を制御するインポート・フィルタと出力経路を制御するエキスポート・フィルタがあります。インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。エキスポート・フィルタは同一ルーティングプロトコル，またはルータ上で同時に動作している異なるプロトコルで学習した経路を広告するかどうかを制御します。フィルタリングの概念を次の図に示します。

図 18-8 フィルタリングの概念

18.4.1 インポート・フィルタ (BGP4+)

インポート・フィルタは指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。インポート・フィルタを指定していない場合は，すべての経路情報を取り込みます。

(1) プリファレンス値

取り込む経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，そのプロトコルのデフォルトのプリファレンス値になります。

同一宛先アドレスの経路情報が複数存在する場合，プリファレンス値によって優先度の高い経路情報が有効となります。プリファレンス値の詳細は，「13.2.3 スタティックルーティングとダイナミックルーティング (BGP4) の同時動作 (1) プリファレンス値」を参照ください。

(2) フィルタリング条件

取り込む経路情報はフィルタリング条件で指定できます。インポート・フィルタのフィルタリング条件を次に示します。

- 送信元ピアアドレス
- 送信元 AS 番号
- 送信元ポリシーグループ番号
- 経路情報の AS_PATH 属性
- 経路情報の ORIGIN 属性

- 経路情報の Community 属性
- 経路情報の宛先ネットワーク

また，取り込まれた経路情報はフィルタリング条件ごとにその経路情報の BGP 属性を変更できます。
フィルタリング条件に付加できる情報を，次に示します。

- LOCAL_PREF 属性
- 追加 AS パス長
- ORIGIN 属性
- MED 属性
- Community 属性

(3) 拡張正規表現

フィルタリング条件である AS_PATH 属性や COMMUNITY 属性は，拡張正規表現 (Extended Regular Expression) によって 1 文字単位に指定できます。拡張正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)（3）拡張正規表現」を参照してください。

(4) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) により複数の AS_PATH に一致するような表現で指定できます。AS パス正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)（4）AS パス正規表現」を参照してください。

(5) MED 属性値

インポート・フィルタと次に示すパラメータの組み合わせによって，学習した BGP4+ 経路情報の MED 属性値を変更できます。

- コンフィグレーションコマンド attribute-list の med サブコマンド
- コンフィグレーションコマンド route-filter の med パラメータ

med サブコマンド (パラメータ) の指定値は，数値指定とオフセット指定があります。

インポート・フィルタと組み合わせた med サブコマンド (パラメータ) でオフセット指定 (±指定) した場合に，学習経路情報に設定される MED 属性値を次の表に示します。

表 18-14　オフセット指定した場合に取り込む経路情報の MED 属性値

学習元プロトコル	MED 属性値
BGP+	• 経路情報に MED 属性値が含まれている場合，経路情報の MED 属性値にオフセット値を±した値を使用します。 • 経路情報に MED 属性値が含まれていない場合，0 を基準にオフセット値を±した値を使用します。

注　オフセット値を±した結果がマイナスになった場合は 0 に，4294967295 を超えた場合は 4294967295 に値が補正されます。

18.4.2　エキスポート・フィルタ (BGP4+)

エキスポート機能はルータ上で同時に動作しているルーティングプロトコル間で経路情報を再配布します。つまり，学習元プロトコルで学習した経路情報を配布先プロトコルを使用して他システム (ルータ) に広告します。

(1) フィルタリング条件

エキスポート・フィルタでは配布先プロトコルのフィルタリング条件 (送出先) と学習元プロトコルのフィルタリング条件 (送出経路情報) によって特定の宛先に特定の経路情報を送出できます。また，配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値となります。

指定できるフィルタリング条件を配布先プロトコルと学習元プロトコルに分け，「表 18-15　配布先プロトコルのフィルタリング条件」と「表 18-16　学習元プロトコルのフィルタリング条件」に示します。なお，配布先プロトコルが，RIPng，または OSPFv3 の場合は，「17.6.2　エキスポート・フィルタ (RIPng/OSPFv3)」を参照してください。

表 18-15　配布先プロトコルのフィルタリング条件

フィルタリング条件 (送出先)	付加情報
• 送信先ピアアドレス • 送信先ポリシーグループ番号 • 送信先 AS 番号	• LOCAL_PREF 属性 • 追加 AS パス長 • ORIGIN 属性 • MED 属性 • Community 属性

表 18-16　学習元プロトコルのフィルタリング条件

学習元プロトコル	フィルタリング条件 (送出経路情報)	備考
RIPng	• 受信インタフェース • 送信元ゲートウェイ • 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIPng で学習された経路情報
OSPF6	• OSPFv3 ドメイン番号 • 経路情報の宛先ネットワーク	OSPFv3 の AS 内経路情報
OSPF6ASE	• OSPFv3 ドメイン番号 • 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPFv3 の AS 外経路情報
BGP4+	• 送信元ピアアドレス • 送信元 AS 番号 • 送信元ポリシーグループ番号 • 経路情報の AS_PATH 属性 • 経路情報の ORIGIN 属性 • 経路情報の Community 属性 • 経路情報の宛先ネットワーク	BGP4+ で学習された経路情報
IS-IS	• 学習元レベル • 経路情報の経路種別 • 経路情報のメトリック種別 • 経路情報の宛先ネットワーク	IS-IS で学習された経路
DIRECT	• インタフェース • 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 送出元インタフェース • 経路情報の宛先ネットワーク	スタティックの経路情報
DEFAULT	• 経路情報の宛先ネットワーク	BGP の DEFAULT 経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

(2) 再配布する経路情報の MED 属性値

再配布する経路情報の MED 属性値を指定するには，次に示すパラメータを使用します。

- エキスポート・フィルタと組み合わせた，コンフィグレーションコマンド attribute-list または route-filter の med サブコマンド (パラメータ)
- コンフィグレーションコマンド bgp4+ の defaultmetric サブコマンド

再配布する経路情報の MED 属性値を「表 18-17　再配布する経路情報の MED 属性値」に示します。また，エキスポート・フィルタと組み合わせた med サブコマンド (パラメータ) でオフセット指定 (±指定) した場合に，再配布する経路情報の MED 属性値を「表 18-18　オフセット指定した場合に再配布する経路情報の MED 属性値」に示します。

表 18-17　再配布する経路情報の MED 属性値

med 指定	学習元プロトコル	MED 属性値
あり	全プロトコル共通	エキスポート・フィルタで指定した MED 属性値を使用します。
なし	BGP4+	外部ピアから学習した経路情報を内部ピアに広告する場合，経路情報の MED 属性値を引き継ぎます。そのほかの場合，コンフィグレーションコマンド attribute-list または route-filter の med サブコマンド (パラメータ) で指定した値を使用します。default-metric サブコマンドの指定がない場合は MED 属性値を設定しません。
	その他	コンフィグレーションコマンド bgp4+ の defaultmetric サブコマンドで指定した値を使用します。default-metric サブコマンドの指定がない場合は MED 属性値を設定しません。

表 18-18　オフセット指定した場合に再配布する経路情報の MED 属性値

学習プロトコル	MED 属性値
全プロトコル共通	「表 18-17　再配布する経路情報の MED 属性値」に示している再配布時に使用する経路情報の MED 属性値に，オフセット値を±した値を使用します。ただし，経路情報に MED 属性値が設定されていない場合は，0 を基準にオフセット値を±した値を使用します。

注　オフセット値を±した結果がマイナスになった場合は 0 に，4294967295 を超えた場合は 4294967295 に値が補正されます。

また，MED 属性値以外に配布先プロトコルに依存する付加情報を配布先のフィルタリング条件ごとに指定できます。指定していない場合は，その配布先プロトコルのデフォルトの値となります。

指定できるフィルタリング条件を配布先プロトコルと学習元プロトコルに分けて「表 18-15　配布先プロトコルのフィルタリング条件」と「表 18-16　学習元プロトコルのフィルタリング条件」に示します。

なお，配布先プロトコルが，RIPng，または OSPFv3 の場合は，「17.6.2　エキスポート・フィルタ (RIPng/OSPFv3)」を参照してください。

(3) 拡張正規表現

フィルタリング条件である AS_PATH 属性や COMMUNITY 属性は，拡張正規表現 (Extended Regular Expression) によって 1 文字単位に指定できます。拡張正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)　(3) 拡張正規表現」を参照してください。

(4) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) によって複

数の AS_PATH に一致するような表現で指定できます。AS パス正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)（4）AS パス正規表現」を参照してください。

(5) エキスポート設定時の注意事項

BGP4+ は同一のルーティングプロトコルで学習した経路情報でも，エキスポートを定義しないと経路情報を広告しないので注意してください。

18.5 経路集約 (BGP4+)

経路集約は一つまたは複数の経路情報から該当する経路情報を包含するようなプレフィックス長のより短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含するような一つの経路情報を生成し，隣接ルータなどに集約経路を通知することによって，ネットワーク上の経路情報の数を少なくする方法です。例えば，3ffe:501:811:ff01::/64 の経路情報や 3ffe:501:811:ff02::/64 の経路情報を学習した場合に 3ffe:501:811:ff::/56 の集約された経路情報を生成するなどです。

経路集約の指定は AGGREGATE(経路集約) コマンドで明示的に指定する必要があります。集約元の経路情報を次の表に示します。

表 18-19　集約元経路情報のフィルタリング条件

集約元プロトコル	フィルタリング条件 (集約元経路情報)	備考
RIPng	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	RIPng で学習された経路情報
OSPF6	• 経路情報の宛先ネットワーク	OSPFv3 の AS 内経路情報
OSPF6ASE	• 経路情報のタグ値 • 経路情報の宛先ネットワーク	OSPFv3 の AS 外経路情報
BGP4+	• 送信元 AS 番号 • 経路情報の AS_PATH 属性 • 経路情報の ORIGIN 属性 • 経路情報の宛先ネットワーク	BGP4+ で学習された経路情報
IS-IS	• 学習元レベル • 経路情報の経路種別 • 経路情報のメトリック種別 • 経路情報の宛先ネットワーク	IS-IS で学習された経路
DIRECT	• 経路情報の宛先ネットワーク	直結インタフェースの経路情報
STATIC	• 経路情報の宛先ネットワーク	スタティックの経路情報
AGGREGATE	• 経路情報の宛先ネットワーク	経路集約によって生成された経路情報

また，集約元経路情報にはフィルタリング条件ごとにその経路情報のプリファレンス値を指定できます。プリファレンス値を指定していない場合は，集約経路のデフォルトのプリファレンス値 (130) が使用されます。なお，集約元の経路情報が学習されていない場合には集約経路情報は生成されません。

(1) AS パス正規表現

フィルタリング条件である AS_PATH 属性は AS パス正規表現 (ASPath-Regular-Expression) により複数の AS_PATH に一致するような表現で指定できます。AS パス正規表現の指定形式は「13.4.1　インポート・フィルタ (BGP4)　(4) AS パス正規表現」を参照してください。

(2) 集約元経路の広告抑止

集約元経路の広告抑止の詳細は，「12.7　経路集約 (RIP/OSPF)　(1) 集約元経路の広告抑止」を参照してください。

(3) 集約経路の転送方法

集約経路によるパケット転送方法の詳細は，「12.7　経路集約 (RIP/OSPF)　(2) 集約経路の転送方法」を参照してください。

19 IPv6 マルチキャスト【OP-MLT】

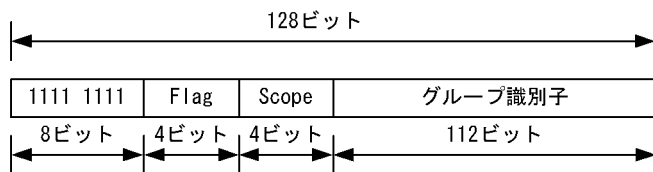
この章では IPv6 マルチキャストの機能について説明します。

19.1　IPv6 マルチキャスト概説

IPv6 マルチキャストは IPv4 マルチキャストと同様の機能を IPv6 で実現します。IPv4 マルチキャストについては，「15.1　IPv4 マルチキャスト概説」を参照してください。IPv4 マルチキャストと IPv6 マルチキャストとは完全に独立に動作します。このため，同一ルータ内でも IPv4 マルチキャストと IPv6 マルチキャストとは全く独立なものとして設定できます。

19.1.1　IPv6 マルチキャストアドレス

IPv6 マルチキャスト通信では上位 8 ビットが FF(16 進数）となる IPv6 アドレスを宛先アドレスとして使用します。IPv6 マルチキャストアドレスはマルチキャストデータの送受信に参加しているグループの間だけの，論理的なグループアドレスです。IPv6 マルチキャストアドレスのフォーマットを次の図に示します。

図 19-1　マルチキャストアドレスのフォーマット

19.1.2　IPv6 マルチキャストのインタフェース種別

本装置の IPv6 マルチキャストのインタフェース種別を次の表に示します。IPv4 マルチキャストとは異なり，マルチホーム構成もサポートされています。

表 19-1　IPv6 マルチキャストのインタフェース種別

インタフェース種別		サポート
LAN	イーサネット	○※1
	Tag-VLAN 連携	○
	リンクアグリゲーション	○
	VLAN	○
	Private VLAN	×
POS		○
共用アドレスインタフェース		×
RM イーサネット (SB-5400S ではリモートマネージメントポート）		×
RM シリアル接続		×
装置 IPv6 アドレス		×※2
ローカルループバックインタフェース		×
Null インタフェース		×
トンネルインタフェース		×

（凡例）　○：使用できる　×：使用できない

注※ 1

Ethernet V2 フレームタイプだけサポートする。

注※ 2

マルチキャスト中継はできないが，ランデブーポイント候補および BSR 候補アドレスとして使用するため，定義は必須になる。

19.1.3 IPv6 マルチキャストルーティング機能

本装置は受信した IPv6 マルチキャストパケットを IPv6 マルチキャスト中継エントリに従って中継します。IPv6 マルチキャストルーティング機能は大きく分けて次の三つの機能から構成されます。

- IPv6 マルチキャストグループマネージメント機能
  IPv6 グループメンバーシップ情報の送受信を行い IPv6 マルチキャストグループの存在を学習する機能です。本装置では MLD(Multicast Listener Discovery) プロトコルを使用します。
- IPv6 経路制御機能
  経路情報を送受信して中継経路を決定し，IPv6 マルチキャスト経路情報および IPv6 マルチキャスト中継エントリを作成する機能です。経路情報収集には PIM-SM(PIM-SSM を含む) を使用します。
- IPv6 中継機能
  IPv6 マルチキャストパケットを IPv6 マルチキャスト中継エントリに従いハードウェアおよびソフトウェアで中継する機能です。
  本装置の IPv6 マルチキャスト中継機能を QoS 機能やフィルタ機能などと併用することによって，IPv6 マルチキャストに QoS 機能を持たせたり不要なパケットをフィルタリングしたりすることもできます。

19.2　IPv6 マルチキャストグループマネージメント機能

IPv6 マルチキャストグループマネージメント機能とは，ルータ - ホスト間での IPv6 グループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上の IPv6 マルチキャストグループメンバの存在を学習する機能です。本装置では IPv6 マルチキャストグループマネージメント機能実現のために MLD をサポートしています。

19.2.1　MLD の概要

MLD はルータ - ホスト間で使用される IPv6 マルチキャストグループ管理プロトコルで，IPv4 マルチキャストの IGMP と同様の機能を持っています。

MLD を使用すると，ルータからの IPv6 マルチキャストグループの参加問い合わせとホストからの IPv6 マルチキャストグループへの参加・離脱報告によって，ルータはホストの IPv6 マルチキャストグループへの参加・離脱を認識して IPv6 マルチキャストパケットを中継・遮断します。通信に使用するアドレスに IPv6 アドレスを使用する点以外は，IGMP とまったく同じです。

MLD はバージョン 1 とバージョン 2 が RFC で規定されています。

MLDv2 は IPv6 マルチキャストグループマネージメント機能を実現する MLDv1 を拡張したプロトコルで，指定した送信元からのマルチキャストパケットだけを受信する送信元フィルタリング機能が導入されています。IPv6 マルチキャストグループへの参加・離脱報告時に送信元指定が可能であるため，MLDv2 と PIM-SSM と組み合わせて使用することで，効率のよい IPv6 マルチキャスト中継が実現できます。

本装置が送信する MLDv1 メッセージのフォーマットおよび設定値は RFC2710 に従います。また，MLDv2 メッセージのフォーマットおよび設定値は RFC3810 に従います。

19.2.2　MLD の動作

（1） MLDv1 の動作

MLD メッセージを次の表に示します。

表 19-2　MLDv1 メッセージ

タイプ		意味	サポート	
			送信	受信
Multicast Listener Query	General Query	IPv6 マルチキャストグループの参加問い合わせ (全グループ宛て)	○	○
	Group-Specific Query	IPv6 マルチキャストグループの参加問い合わせ (特定グループ宛て)	○	○
Multicast Listener Report		加入している IPv6 マルチキャストグループの報告	×	○
Multicast Listener Done		IPv6 マルチキャストグループからの離脱報告	×	○

(凡例)　○：サポートする　×：サポートしない

(2) MLDv2 の動作

MLDv2 はフィルタモードと送信元リストを指定することで，送信元フィルタリング機能を実現します。フィルタモードには次の二つのモードがあります。

- INCLUDE：指定された送信元リストからのパケットだけ中継します
- EXCLUDE：指定された送信元リスト以外からのパケットだけ中継します

MLDv2 メッセージを次の表に示します。

表 19-3 MLDv2 メッセージ

タイプ		意味	サポート	
			送信	受信
Version 2 Multicast Listener Query	General Query	IPv6 マルチキャストグループの参加問い合わせ（全グループ宛て）	○	○
	Multicast Address Specific Query	IPv6 マルチキャストグループの参加問い合わせ（特定グループ宛て）	○	○
	Multicast Address and Source Specific Query	IPv6 マルチキャストグループの参加問合せ（特定の送信元およびグループ宛て）	○	○
Version 2 MulticastListener Report	Current StateReport	加入している IPv6 マルチキャストグループとフィルタモード報告	×	○
	State ChangeReport	加入している IPv6 マルチキャストグループとフィルタモードの更新報告	×	○

（凡例） ○：サポートする　×：サポートしない

フィルタモードおよび送信元リストはグループ加入後に変更することが可能で，Report メッセージに含まれる Multicast Address Record で指定します。本装置がサポートする Multicast Address Record タイプを次の表に示します

表 19-4 Multicast Address Record タイプ

タイプ		意味	サポート
Current State Report	MODE_IS_INCLUDE	INCLUDE モードであることを示します	○
	MODE_IS_EXCLUDE	EXCLUDE モードであることを示します	○ （送信元リストは無視します）
State Change Report	CHANGE_TO_ INCLUDE_MODE	フィルタモードを INCLUDE に変更することを示します	○
	CHANGE_TO_ EXCLUDE_MODE	フィルタモードを EXCLUDE に変更することを示します	○ （送信元リストは無視します）
	ALLOW_NEW_ SOURCES	データの受信を希望する送信元を追加することを示します	○
	BLOCK_OLD_ SOURCES	データの受信を希望する送信元を削除することを示します	○

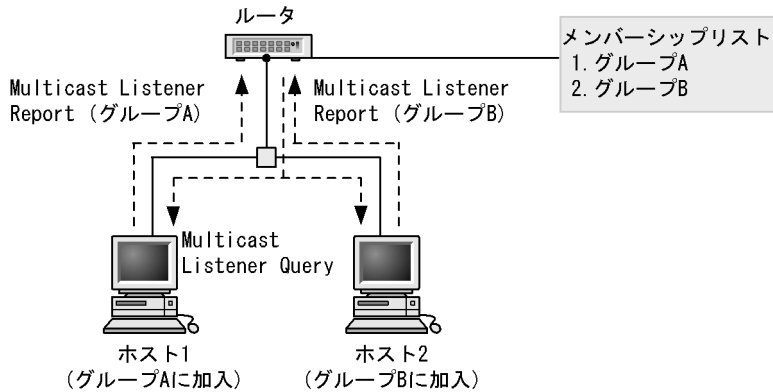
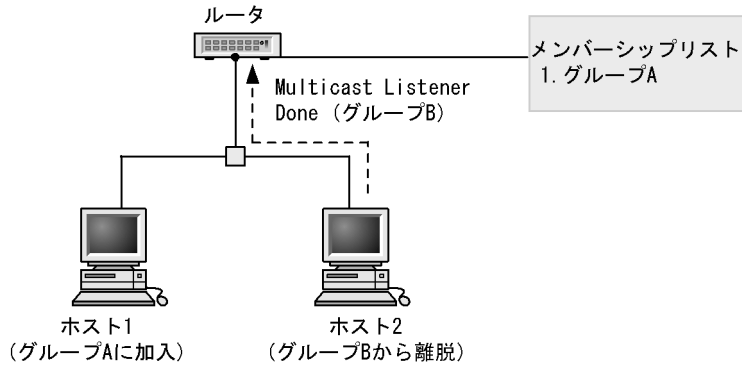
（凡例）　○：サポートする

MLDv1 メッセージを使用した MLDv1 の動作を次に示します。

- IPv6 マルチキャストルータは，直接接続するインタフェース上に IPv6 マルチキャストメンバーシップの情報を得るために，定期的に Multicast Listener Query メッセージをリンクローカル・全ノードアドレス ff02::1 宛てに送信します。
- ホストから Multicast Listener Report を受信すると，IPv6 マルチキャストルータはメンバーシップリストにそのグループを追加します。
- Multicast Listener Done メッセージを受信するとそのグループをメンバーシップリストから削除します。

MLDv1 グループ参加・離脱動作を次の図に示します。

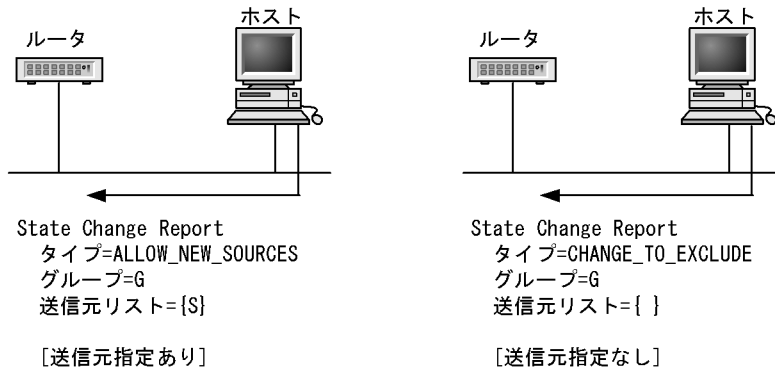
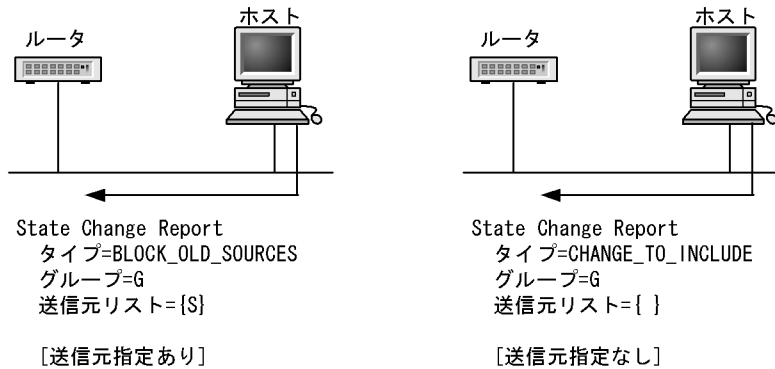
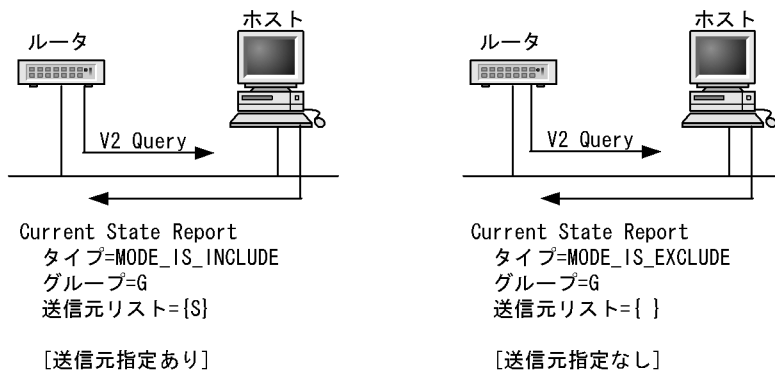
図 19-2　MLDv1 グループ参加・離脱動作

●ホスト1がグループA，ホスト2がグループBに加入する場合

●ホスト2がグループBから離脱する場合

MLDv2 メッセージを使用した MLDv2 の動作を次に示します。

- IPv6 マルチキャストルータは，直接接続するインタフェース上に IPv6 マルチキャストメンバーシップの情報を得るために，定期的に Version 2 Multicast Listener Query (General Query) メッセージをリンクローカル・全ノードアドレス ff02::1 宛てに送信します。
- ホストは Version 2 Multicast Report (State Change Report および Current State Report) を ff02::16 宛てに送信します。
- ホストから Version 2 Multicast Listener Report (State Change Report) メッセージを受信すると IPv6 マルチキャストルータは Multicast Address Record タイプの内容に応じてメンバーシップリストへのグループ追加，あるいはメンバーシップリストからのグループ削除を行います。

- ホストは Version 2 Multicast Listener Query を受信すると，グループへの参加状況を Version 2 Multicast listener Report (Current State Report) で応答します。

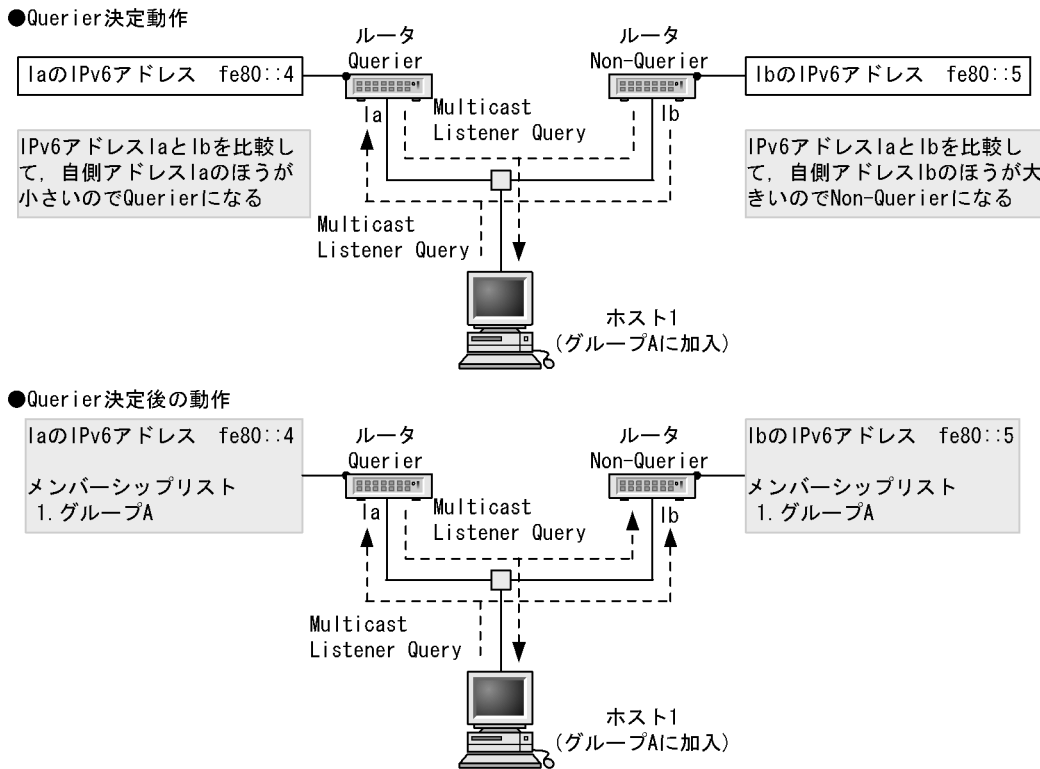
ホストからの MLDv2 Report メッセージ送信動作を次の図に示します。

図 19-3　MLDv2 グループ参加・離脱動作

19.2.3　Querier の決定

MLD ルータは Querier か Non-Querier のどちらか一方の役割を果たします。同一ネットワーク上に複数のルータが存在する場合，そのうちの一つが定期的な Multicast Listener Query メッセージを送信する Querier になります。

Querier を決定するには，同一ネットワーク上に存在する MLD ルータから受信した Multicast Listener Query の送信元 IPv6 リンクローカルアドレスと自インタフェースの IPv6 リンクローカルアドレスを比較します。自インタフェースの方が小さければ Querier として動作します。自インタフェースの方が大きければ Non-Querier となり，Multicast Listener Query は送信しません。

この動作によって同一ネットワーク上には Querier は一つだけ存在することになります。Querier と Non-Querier の決定を次の図に示します。

図 19-4　Querier と Non-Querier の決定

Querier になった場合，送信元 IPv6 アドレスが自インタフェースより小さい Multicast Listener Query を受信するまで Querier として動作して，Multicast Listener Query を定期的（デフォルト値 125 秒）に送信します。Non-Querier が Querier として動作するのは次に示す場合です。

- Querier の送信した Multicast Listener Query を監視し，Multicast Listener Query 受信時に Multicast Listener Query の送信元 IPv6 リンクローカルアドレスが自インタフェースのリンクローカルアドレスよりも大きい場合
- Multicast Listener Query を一定時間（デフォルト値 255 秒）受信しなかった場合

インタフェースに定義された IPv6 リンクローカルアドレス以外のアドレスは，Querier の決定には影響しません。

MLDv2 ルータは MLDv1 ルータと同じ方法で Querier を決定します。

19.2.4 IPv6 グループメンバの管理

（1） MLDv1 使用時の IPv6 グループメンバ管理

MLDv1 使用時の IPv6 グループメンバの登録および削除について説明します。

ホストから Multicast Listener Report を受信することで IPv6 グループメンバを登録します。なお，Non-Querier でもホストからの Multicast Listener Report を受信することによって Querier 同様に IPv6 グループメンバを登録します。

Querier が，ホストからある IPv6 グループへの離脱報告である Multicast Listener Done メッセージを受信した場合，離脱報告を受けたグループメンバに参加しているそのほかのホストの存在を確認するために，該当するグループ宛てに Multicast Listener Query(Group-Specific Query) メッセージを連続して (1 秒間隔) 送信します。このメッセージを 2 回送信したあと，Multicast Listener Report を 1 秒間受信しない場合，該当するグループを削除します。なお，Non-Querier の場合は Multicast Listener Done メッセージを無視し，Querier が送信した Multicast Listener Query(Group-Specific Query) メッセージを 2 回受信したあと Multicast Listener Report を 1 秒間受信しない場合，該当するグループを削除します。

（2） MLDv2 使用時の IPv6 グループメンバ管理

MLDv2 使用時の IPv6 グループメンバの登録および削除について説明します。

ホストからマルチキャストグループへの加入要求を示す Report を受信することでグループ情報を登録します。ここでグループ情報とは，グループアドレスと当該グループアドレスへの送信元アドレスを指します。Querier，Non-Querier ともに Report を受信することでグループ情報を登録します。

Querier は，マルチキャストグループからの離脱要求を示す Report を受信すると，当該グループメンバに参加しているほかのホストの存在を確かめるために，送信元リストの指定有無に応じて次に示すメッセージを 1 秒間隔で送信します。

- 送信元リスト指定無し：Multicast Address Specific Query メッセージ
- 送信元リスト指定有り：Multicast Address and Source Specific Query メッセージ

本装置が Query の場合は上記のメッセージを 2 回送信後，1 秒間 Report を受信しない場合該当するグループ情報を削除します。本装置が Non-Querier の場合は Querier 送信する上記メッセージを受信後，該当するグループ情報の削除処理を実行します。

19.2.5 MLD タイマ値

本装置が使用する MLDv1 タイマ値を次の表に示します。

表 19-5 MLDv1 タイマ値

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Query Interval	Multicast Listener Query 送信周期時間	125	60 ～ 3,600	-
Query Response Interval	Multicast Listener Report 最大応答待ち時間	10	-	-
Other Querier Present Interval	Querier 監視時間	255	Query interval × 2 + QueryResponse Interval / 2	左記計算式より算出。
Startup Query Interval	Startup 時 GenaralQuery を送信する時間	32	Query Interval / 4	左記計算式より算出。

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Last Member Query Interval	Done 受信後の Specific Query 送信周期	1	-	-
Multicast Listener Interval	グループメンバの保持時間	260	Query interval × 2 + QueryResponse Interval	左記計算式より算出。

(凡例) - : 該当しない

本装置が使用する MLDv2 タイマ値を次の表に示します。

表 19-6 MLDv2 タイマ値

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Query Interval	Multicast Listener Query 送信周期時間	125	60 〜 3,600	-
Query Response Interval	Multicast Listener Report 最大応答待ち時間	10	-	-
Other Querier Present Interval	Querier 監視時間	255	Query Interval × 2 + QueryResponse Interval / 2	左記計算式より算出。
Startup Query Interval	Startup 時 General Query を送信する時間	30	Query Interval / 4	左記計算式より算出。
Last Listener Query Interval	離脱要求 受信後の Specific Query 送信周期	1	-	-
Multicast Address Listening Interval	グループメンバの保持時間	260	Query Interval × 2 + Query Response Interval	左記計算式より算出。
Older Version Host Present Interval	MLDv2 マルチキャストアドレス互換モードへの移行時間	260	Query Interval × 2 + Query Response Interval	左記計算式より算出。

(凡例) - : 該当しない

19.2.6 MLDv1/MLDv2 装置との接続

本装置は MLDv1 と MLDv2 をサポートします。コンフィグレーションの mld コマンドで，インタフェースごとに使用する MLD バージョンを設定できます。指定するバージョンに応じた動作を次の表に示します。デフォルトは version 1 です。

表 19-7 MLD バージョン指定時の動作

指定バージョン	バージョン指定時の動作
version 1	MLDv1 で動作します。 MLDv2 パケットは無視します。
version 2	MLDv1,MLDv2 の両方で動作可能です。 MLDv1，MLDv2 それぞれグループアドレス単位で動作します。
version 2 only	MLDv2 で動作します。 MLDv1 パケットは無視します。

（1） MLDv1/MLDv2 ルータとの接続

冗長構成などによって同一ネットワーク上に複数の MLD ルータが存在する場合，互いの Query を受信することで Querier を決定します（「19.2.3 Querier の決定」を参照してください）。本装置は，MLD バージョンが version 2 あるいは version 2 only に設定されているインタフェースでの MLDv1 ルータとの接続はサポートしません (V1 Query を無視するため，Querier を決定できなくなります)。MLDv1 ルータと接続する場合は，当該インタフェースの MLD バージョンを version 1 に設定してください。

（2） MLDv1/MLDv2 ホストとの接続

MLDv1 ホストと MLDv2 ホストが混在するネットワークと接続する場合は，当該インタフェースの MLD バージョンを version 2 に設定してください。ただし，MLDv1 ホストは MLDv2 Query を MLDv1 Query として受信できる (RFC 仕様) ことが必要になります。

MLDv1/MLDv2 ホストが混在する場合，グループメンバの登録はグループ加入を要求する MLD のバージョンによって次の表に従います。

表 19-8 MLDv1/MLDv2 ホスト混在時のグループメンバ登録

グループ加入の要求	グループメンバの登録
MLDv1 で受信	MLDv1 モードでグループメンバを登録
MLDv2 で受信	MLDv2 モードでグループメンバを登録
MLDv1 と MLDv2 で受信	MLDv1 モードでグループメンバを登録

19.2.7 静的グループ参加

MLD 対応ホストが存在しないネットワークに IPv6 マルチキャストパケットを中継するために，静的グループ参加機能を設定します。

静的グループ参加を設定したインタフェースは，Multicast Listener Rerpot を受信しなくともグループ参加したものと同様の動作を行います。

この機能は MLDv1 の機能のため，当該インタフェースの MLD バージョンを version 2 only に設定している場合は動作しません。また，version 2 に設定されている場合は MLDv1 でグループ参加したものと同様の動作を行います。

19.2.8 MLD 使用時の注意事項

- 構成変更によって静的グループ参加を設定した場合，PIM-SM グループの場合は (*,G) エントリ，PIM-SSM グループの場合は (S,G) エントリが作成されるまで最大 250 秒かかります。
- コンフィグレーションで設定している SSM アドレスの範囲外のグループに対して，送信元指定有りの MLDv2 Report を受信した場合は全送信元からのマルチキャストパケットを中継します。

19.3 IPv6 マルチキャスト中継機能

IPv6 マルチキャストパケットの中継処理は IPv6 マルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで行います。一度中継した IPv6 マルチキャストパケットの中継情報をハードウェアの IPv6 マルチキャスト中継エントリに登録します。登録された IPv6 パケットはハードウェアで中継を行い，登録されていない IPv6 パケットはソフトウェアの IPv6 マルチキャスト経路情報から生成した IPv6 マルチキャスト中継エントリに従って中継を行います。中継対象アドレスについての制限を除き，IPv4 マルチキャスト中継機能とは特別な違いはありません。

19.3.1 中継対象アドレス

IPv6 マルチキャストアドレスのうち，ノードローカル・マルチキャストアドレス (ff01::/16) およびリンクローカル・マルチキャストアドレス (ff02::/16) は IPv6 マルチキャスト中継処理の対象外です。

19.3.2 IPv6 マルチキャストパケット中継処理

IPv6 マルチキャストのパケット中継はハードウェアの中継処理，ソフトウェアの中継処理によって行われます。

(1) ハードウェアの中継処理

ハードウェアによる IPv6 マルチキャストのパケット中継処理は次に示す四つの手順で実行されます。

1. IPv6 マルチキャスト中継エントリの検索
   IPv6 マルチキャストグループ宛てのパケットを受信した場合，ハードウェアの IPv6 マルチキャスト中継エントリから該当エントリを検索します。
2. パケット受信インタフェースの正常性チェック
   1 の手順でエントリが存在した場合，その IPv6 パケットが正しいインタフェースから受信されているかどうかをチェックします。
3. フィルタリング
   IPv6 フィルタリングテーブルに登録された情報を参照して中継するかどうかを判断します。
4. ホップリミットに基づいた中継判断と TTL 値のデクリメント
   パケット中のホップリミット値から中継するかを判断し，中継する場合は該当するパケットのホップリミット値をデクリメントします。

(2) ソフトウェアの中継処理

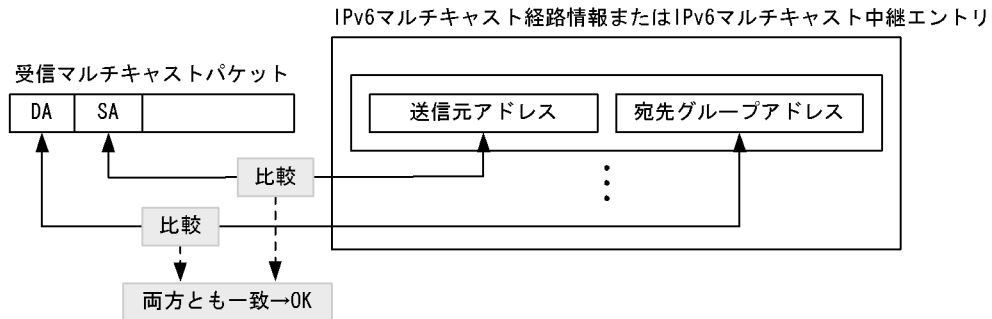
ソフトウェアによる IPv6 マルチキャストパケット中継処理は次に示す場合ごとに処理が異なります。

- ハードウェアの IPv6 マルチキャスト中継エントリにエントリがない場合
  ある送信元からある IPv6 マルチキャストグループ宛てのパケットを最初に受信した場合，IPv6 マルチキャスト経路情報から生成した中継エントリに従って，ソフトウェアで中継します。同時にハードウェアに対して IPv6 マルチキャスト中継エントリを登録します。
- IPv6 カプセル化処理を行う場合
  一時的にランデブーポイント宛てに IPv6 カプセル化を行って中継し，ランデブーポイントでは各中継先にカプセル化を解除して中継します。

(3) IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリの検索

受信した IPv6 マルチキャストパケットの DA(宛先グループアドレス) と SA(送信元アドレス) に該当す

るエントリを IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリから検索します。
IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリの検索方法を次の図に示します。

図 19-5　IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリの検索方法

19.3.3　ネガティブキャッシュ

ネガティブキャッシュは，中継できないマルチキャストパケットをハードウェアによって廃棄する機能です。ネガティブキャッシュは中継先インタフェースの存在しない中継エントリです。ネガティブキャッシュは，中継できないマルチキャストパケットを受信すると，ハードウェアに登録します。その後，登録したマルチキャストパケットと同じアドレスのマルチキャストパケットを受信すると，そのパケットをハードウェアによって廃棄します。これによって，大量の中継できないマルチキャストパケットを受信しても，それを原因とする負荷上昇を抑えられます。

19.4 IPv6 経路制御機能

IPv6 経路制御機能とは，IPv6 マルチキャストルーティングプロトコルを使用して収集した隣接情報やグループ情報を基に，IPv6 マルチキャスト経路情報および IPv6 マルチキャスト中継エントリを作成する機能です。本装置は IPv6 マルチキャストルーティングプロトコルとして PIM-SM をサポートしています。

IPv6 PIM-SM は IPv4 PIM-SM を IPv6 対応させたものです。IPv4 PIM-SM 概要については，「15.4.2 IPv4 PIM-SM」をご参照ください。なお IPv6 PIM-SM は IPv4 PIM-SM とは独立に動作するので，IPv4 PIM-SM と IPv6 PIM-SM は独立して設定できます。

同一ネットワーク内で IPv6 マルチキャストパケットの中継を行う場合は，すべてのルータで同じ IPv6 マルチキャストプロトコルが動作するように設定してください。同一ネットワーク内に IPv6 PIM-DM が動作しているルータ，IPv6 PIM-SM が動作しているルータが混在している場合，各ルータ間で IPv6 マルチキャストパケットの中継は行われません。

本装置が送信する IPv6 PIM-SM フレームのフォーマットおよび設定値は RFC2362 に従います。

19.4.1 IPv6 PIM-SM の動作

IPv6 PIM-SM メッセージのサポート仕様を次の表に示します。すべてのメッセージが送信および受信をサポートしています。

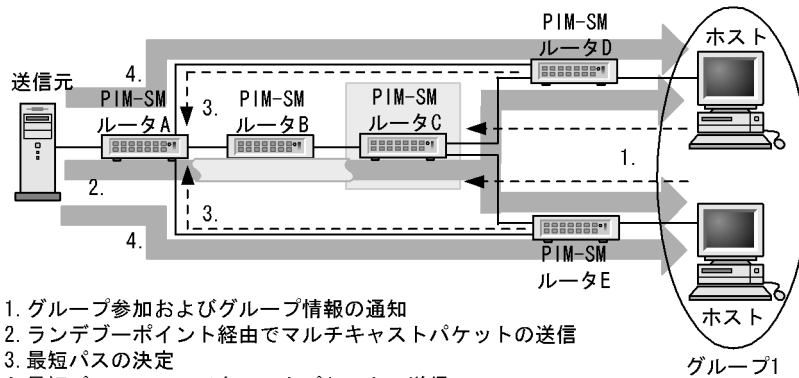
表 19-9 IPv6 PIM-SM メッセージのサポート仕様

タイプ	機能
PIM-Hello	PIM 近隣ルータの検出
PIM-Join ／ Prune	マルチキャスト配送ツリーの参加および刈り込み
PIM-Assert	Forwarder の決定
PIM-Register	マルチキャストパケットをランデブーポイント宛てにカプセル化する。
PIM-Register-stop	Register メッセージを抑止する。
PIM-Bootstrap	BSR を決定する。またランデブーポイントの情報を配信する。
PIM-Candidate-RP-Advertisement	ランデブーポイントが BSR に自ランデブーポイント情報を通知する。

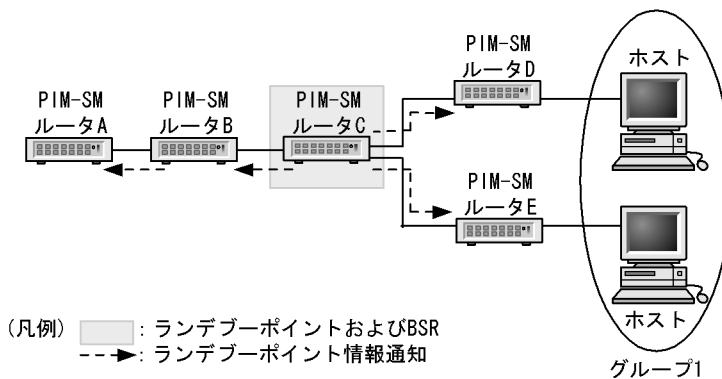
IPv6 PIM-SM の動作の流れを次に示します。

1. 各 IPv6 PIM-SM ルータは MLD で学習したグループ情報をランデブーポイントに通知します。
2. ランデブーポイントは各 IPv6 PIM-SM からグループ情報の受信で各グループの存在を認識します。
3. IPv6 PIM-SM は最初にマルチキャストパケットをその送信元ネットワークからランデブーポイント経由ですべてのグループメンバに配送するために，送信元を頂点としたランデブーポイント経由配送ツリーを形成します。
4. 送信元から各グループに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信元からの最短パスを決定します (最短パス配送ツリーを形成します)。
5. 送信元から最短パスで各グループメンバへのマルチキャストパケット中継を行います。

PIM-SM の動作概要を次の図に示します。

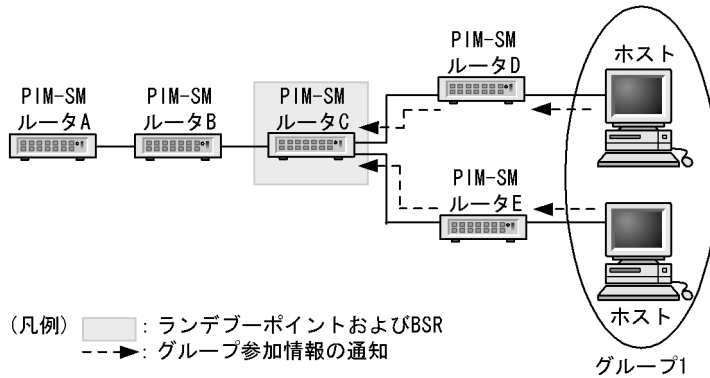
図 19-6　PIM-SM の動作概要

(1)　ランデブーポイントおよびブートストラップルータ (BSR)

ランデブーポイントルータおよび BSR はコンフィグレーションで定義します。BSR はランデブーポイントの情報 (IPv6 アドレスなど) をすべてのマルチキャストインタフェースに通知します。この通知はホップバイホップで全 PIM ルータリンクローカル・マルチキャストアドレス (ff02::d) 宛てに行われます。ランデブーポイントおよびブートストラップルータ (BSR) を次の図に示します。

図 19-7　ランデブーポイントおよびブートストラップルータ (BSR)

BSR(PIM-SM ルータ C) はランデブーポイント情報をすべての IPv6 マルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IPv6 アドレスを学習し，受信したインタフェース以外で IPv6 PIM ルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

(2)　ランデブーポイントに対するグループ参加情報の通知

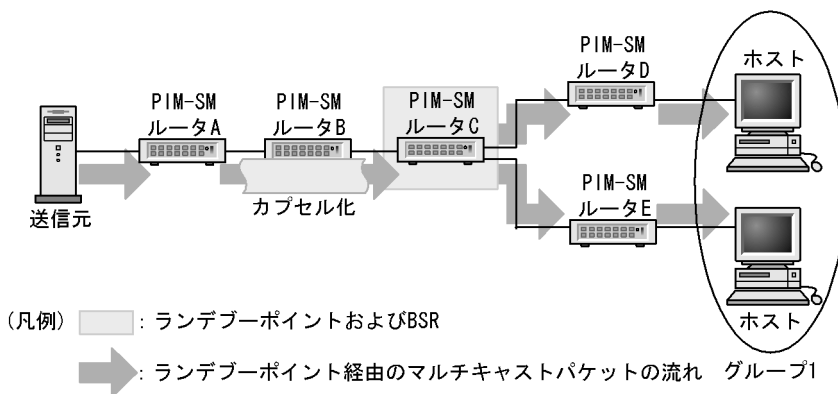
各ルータは MLD で学習したグループ参加情報をランデブーポイントに通知します。この通知のときに使用される送信元および宛先 IPv6 アドレスは，それぞれ該当するルータの装置アドレスになります。ランデブーポイントは IPv6 グループ情報を受信することで，IPv6 グループの存在をインタフェースごとに認識します。ランデブーポイントに対するグループ参加情報の通知を次の図に示します。

図 19-8　ランデブーポイントへのグループ参加情報の通知

まず，各ホストは MLD でグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はグループ 1 情報を学習し，ランデブーポイント (PIM-SM ルータ C) にグループ 1 情報を通知します。ランデブーポイント (PIM-SM ルータ C) はグループ 1 情報を受信することによって受信したインタフェースにグループ 1 が存在することを学習します。

(3)　IPv6 マルチキャストパケット通信 (カプセル化)

送信元のサーバがグループ 1 宛ての IPv6 マルチキャストパケットを送信した場合，PIM-SM ルータ A はその IPv6 マルチキャストパケットをランデブーポイント (PIM-SM ルータ C) 宛てに IPv6 カプセル化 (Register パケット) して送信します。本装置の場合，この通知のときに使用される送信元および宛先 IPv6 アドレスは，それぞれ該当するルータの装置アドレスになります (ランデブーポイントの IPv6 アドレスは「(1)　ランデブーポイントおよびブートストラップルータ (BSR)」で学習済み)。

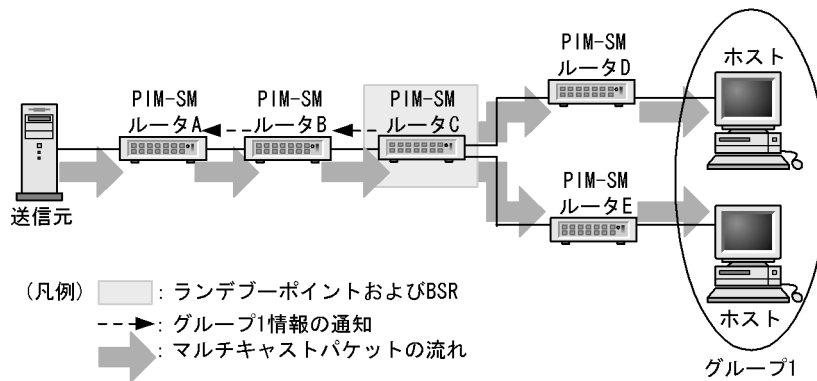
ランデブーポイント (PIM-SM ルータ C) は IPv6 カプセル化したパケットを受信すると，非カプセル化を解除してグループ 1 が存在するインタフェースにグループ 1 宛てのマルチキャストパケットを中継します (グループ 1 の存在は「(2)　ランデブーポイントに対するグループ参加情報の通知」で学習済み)。
PIM-SM ルータ D および PIM-SM ルータ E は，グループ 1 宛ての IPv6 マルチキャストパケットを受信すると，グループ 1 が存在するインタフェースに IPv6 マルチキャストパケットを中継します (グループ 1 の存在は「(2)　ランデブーポイントに対するグループ参加情報の通知」の MLD で学習済み)。IPv6 マルチキャストパケット通信 (カプセル化) を次の図に示します。

図 19-9　IPv6 マルチキャストパケット通信 (カプセル化)

(4) IPv6 マルチキャストパケット通信 (カプセル化の解除)

ランデブーポイント (PIM-SM ルータ C) は IPv6 カプセル化したパケットを受信すると，カプセル化を解除してグループ 1 が存在するインタフェースにグループ 1 宛ての IPv6 マルチキャストパケットを中継します (「(3) IPv6 マルチキャストパケット通信 (カプセル化)」で説明)。

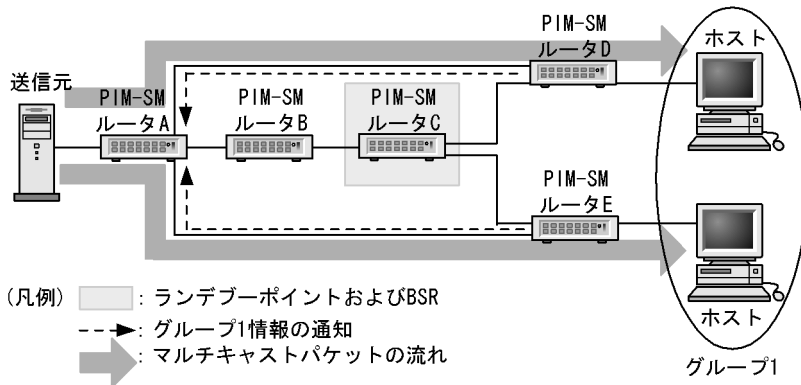
ランデブーポイントはこの処理のあと，既存の IPv6 ユニキャストルーティング情報を基に決定された送信元のサーバの方向にグループ 1 情報を通知します。この通知のときに使用される宛先アドレスは全 PIM ルータリンクローカル・マルチキャストアドレス (ff02::d) です。

グループ 1 情報を受信した PIM-SM ルータ B および PIM-SM ルータ A は受信したインタフェースのグループ 1 の存在を認識 (学習) します。PIM-SM ルータ A は送信元サーバが送信したグループ 1 宛ての IPv6 マルチキャストパケットを IPv6 カプセル化しないで該当するインタフェースに中継します。グループ 1 宛ての IPv6 マルチキャストパケットを受信した PIM-SM ルータ B，PIM-SM ルータ C，PIM-SM ルータ D，PIM-SM ルータ E はグループ 1 が存在するインタフェースに中継します。IPv6 マルチキャストパケット通信 (非カプセル化) を次の図に示します。

図 19-10　IPv6 マルチキャストパケット通信 (非カプセル化)

(5) 最短パスのマルチキャストパケット通信

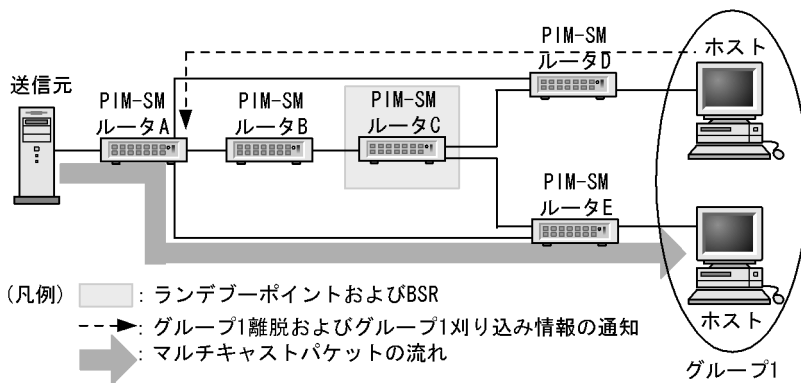
PIM-SM ルータ D および PIM-SM ルータ E は，送信元サーバのグループ 1 宛て IPv6 マルチキャストパケットを受信した場合 (「(3) IPv6 マルチキャストパケット通信 (カプセル化)」で説明)，PIM-SM ルータ D および PIM-SM ルータ E は送信元サーバに対して最短のパス (既存の IPv6 ユニキャストルーティング情報) の方向にグループ 1 情報を通知します。この通知のときに使用される宛先アドレスは全 PIM ルータリンクローカル・マルチキャストアドレス (ff02::d) です。

PIM-SM ルータ A は，PIM-SM ルータ D および PIM-SM ルータ E からグループ 1 情報を受信すると，受信したインタフェースにグループ 1 の存在を認識し，送信元サーバのグループ A 宛ての IPv6 マルチキャストパケットを受信すると該当するインタフェースに中継します。最短パスの IPv6 マルチキャストパケット通信を次の図に示します。

図 19-11　最短パスの IPv6 マルチキャストパケット通信

(6) IPv6 マルチキャスト配送ツリーの刈り込み

PIM-SM ルータ D は，ホストが MLD でグループ A から離脱をした場合，グループ 1 情報を通知していたインタフェースに対してグループ 1 の刈り込み情報を通知します。この通知のときに使用される宛先アドレスは全 PIM ルータリンクローカル・マルチキャストアドレス (ff02::d) です。

PIM-SM ルータ A はグループ 1 の刈り込み通知を受信すると，受信したインタフェースに対してグループ 1 宛ての IPv6 マルチキャストパケットの中継を中止します。IPv6 マルチキャスト配送ツリーの刈り込みを次の図に示します。

図 19-12　IPv6 マルチキャスト配送ツリーの刈り込み

19.4.2　近隣検出

IPv6 PIM ルータは IPv6 PIM を有効にしたすべてのインタフェースに定期的に IPv6 PIM-Hello メッセージを送信します。PIM-Hello メッセージの送信先は全 PIM ルータリンクローカル・マルチキャストアドレス宛て (ff02::d) です。このメッセージを受信することによって近隣の IPv6 PIM ルータを動的に検出します。

本装置は PIM-Hello メッセージの Generation ID オプションをサポートしています（RFC4601 および draft-ietf-pim-sm-bsr-07.txt に準拠）。

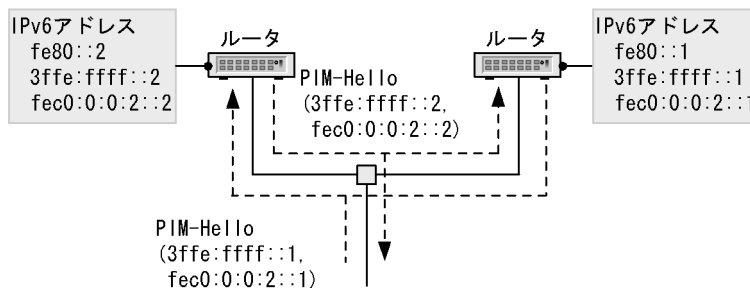
Generaion ID はマルチキャストインタフェースごとに持つ 32 ビットの乱数で，PIM-Hello メッセージ送信時に Generation ID を付加して送信します。Generation ID はマルチキャストインタフェースが Up 状態になるたびに再生成します。受信した PIM-Hello メッセージに Generation ID オプションが付加されて

いれば Generation ID を記憶し，Generation ID の変化によって近隣装置のインタフェース障害を検出します。Generation ID の変化を検出すると，近隣装置情報の更新と PIM-Hello メッセージ，PIM Bootstrap メッセージ，および PIM Join/Prune メッセージを定期広告のタイミングを待たずに送信します。これによって，マルチキャスト経路情報を速やかに再学習することができます。

本装置から送信される PIM-Hello メッセージには，送信元インタフェースに定義されているリンクローカルアドレス以外のアドレスリストが PIM-Hello メッセージのオプションデータ (タイプ 24 およびタイプ 65001) として含まれています。このオプションデータを受信することによって，本装置は隣接する IPv6 PIM ルータのリンクローカルアドレス以外のアドレスを認識できます。

本装置から IPv6 マルチキャスト送信者へ到達するためのネクストホップがリンクローカルアドレス以外の場合にも，このアドレスリストを参照することによって本装置は送信者へ到達するための IPv6 PIM ルータを検出できます。

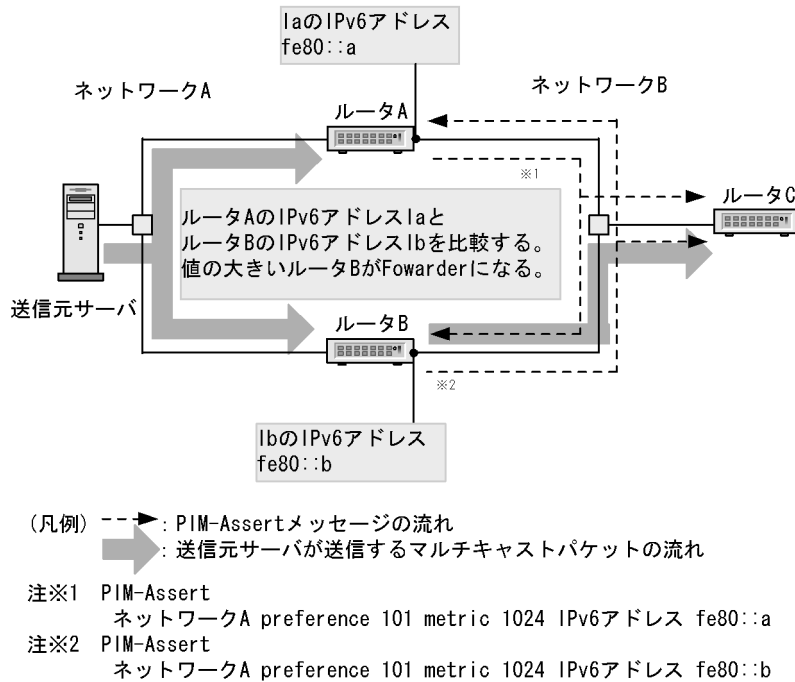
隣接 PIM ルータのアドレス受信例を次の図に示します。

図 19-13　PIM-Hello メッセージによる隣接ルータアドレス受信

19.4.3　Forwarder の決定

同一 LAN 上に複数の IPv6 PIM ルータが接続している場合，そのネットワークに重複パケットがフォワードされる可能性があります。IPv6 PIM ルータは同一 LAN 上に複数の IPv6 PIM ルータが存在した場合，PIM-Assert メッセージに含まれるメトリックを参照し，送信元ネットワークに対して最も小さいメトリックを持ったルータが同一 LAN 上にパケットをフォワードする権利を持ちます。もしメトリックが等しい場合，より大きい IPv6 リンクローカルアドレスを持ったルータがフォワードする権利を持ちます。Forwarder の決定を次の図に示します。

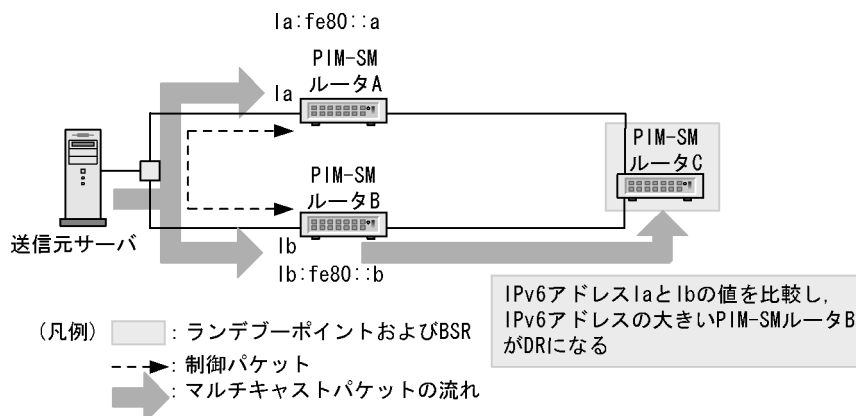
図 19-14 Forwarder の決定

（凡例）- - -▶：PIM-Assertメッセージの流れ
：送信元サーバが送信するマルチキャストパケットの流れ

注※1 PIM-Assert
ネットワークA preference 101 metric 1024 IPv6アドレス fe80::a
注※2 PIM-Assert
ネットワークA preference 101 metric 1024 IPv6アドレス fe80::b

19.4.4 DR の決定および動作

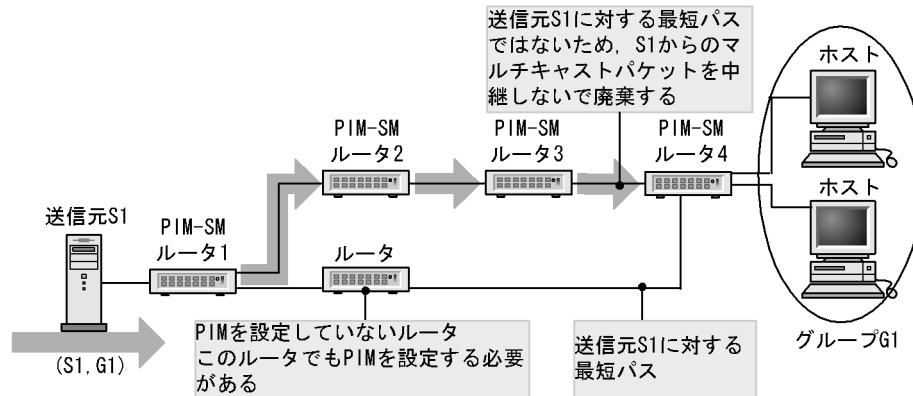
同一 LAN 上で複数の IPv6 PIM-SM ルータが存在する場合，送信元が送信した IPv6 マルチキャストパケットをランデブーポイントに IPv6 カプセル化して中継するルータ（DR）を決定します。DR はそのインタフェース上で一番大きい IPv6 リンクローカルアドレスのルータが DR になります。例えば，ルータ A とルータ B の IPv6 リンクローカルアドレスを比較してルータ B の方が IPv6 リンクローカルアドレスが大きい場合，ルータ B が DR となってランデブーポイントに対して IPv6 カプセル化パケットを中継します。DR の動作を，次の図に示します。

図 19-15 DR の動作

（凡例） ：ランデブーポイントおよびBSR
- - -▶：制御パケット
：マルチキャストパケットの流れ

19.4.5 冗長経路時の注意事項

次に示す図のような冗長構成の場合，IPv6 マルチキャストパケットがフォワードされないので注意してく

ださい。冗長経路がある場合は，その経路上のすべてのルータで IPv6 PIM-SM の設定が必要になります。

図 19-16　冗長経路時の注意事項

19.4.6　IPv6 PIM-SM タイマ仕様

IPv6 PIM-SM タイマ値を次の表に示します。

表 19-10　IPv6 PIM-SM タイマ値

タイマ名	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Hello-Period	Hello の送信周期	30	10 〜 3,600	-
Hello-Holdtime	隣接関係の保持期間	105	3.5 × Hello-Period	左記計算式より算出。
Assert-Timeout	Assert による中継抑止期間	180	-	-
Join/Prune-Period	Join/Prune の送信周期	60	30 〜 3,600	最大で +50% の揺らぎが生じます。
Join/Prune-Holdtime	経路情報および中継先インタフェースの保持期間	210	3.5 × Join/Prune-Period	左記計算式より算出。
Deletion-Delay-Time	Prune 受信後のマルチキャスト中継先インタフェースの保持期間	1/3 ×受信した Prune に含まれる保持期間	0 〜 300	※ 1
Data-Timeout	中継エントリの保持期間	210	60 〜 43,200 または無期限	最大で +90 秒の誤差が発生します。
Register-Supression-Timer	カプセル化送信の抑止期間	60	-	最大で± 30 秒の揺らぎが生じます。
Probe-Time	カプセル化送信の再開確認を送信する時間	5	5 〜 60	デフォルトの 5 秒では Register-Supression-Timer が満了する 5 秒前にカプセル化送信の再開確認 (Null-Register) を一度だけ送信します。※ 2
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60	-	-

タイマ名	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
RP-Holdtime	ランデブーポイント保持期間	150	2.5 × C-RP-Adv-Period	左記計算式より算出。
Bootstrap-Period	BSR メッセージ送信周期	60	-	-
Bootstrap-Timeout	BSR メッセージの保持期間	130	2 × Bootstrap-Period +10	左記計算式より算出。
Negative-Cache-Holdtime(PIM-SM)	ネガティブキャッシュの保持期間	210	10 ～ 3,600	PIM-SSM の場合は 3,600 秒の固定。

(凡例)　- : 該当しない

注※ 1

本タイマ値はコンフィグレーションで設定された値が優先されるため，RFC2362 の規定とは異なった動作をします。ただし，コンフィグレーションで値を指定していない場合には RFC2362 の動作に準じます。

注※ 2

本タイマ値を 10 以上に設定すると，カプセル化送信の再開確認を 5 秒おきに複数回送信します。コンフィグレーションで値を指定していない場合には，一度だけ送信します。

19.4.7　IPv6 PIM-SM 使用時の注意事項

IPv6 PIM-SM を使用したネットワークを構成する場合には，次に示す制限事項に留意してください。

本装置は RFC2362(PIM-SM 仕様) に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 19-11　RFC との差分

RFC		本装置
パケットフォーマット	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにマスク長を設定するフィールドがある。	エンコードアドレスのマスク長は 128 固定。
	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにアドレスファミリーとエンコードタイプを設定するフィールドがある。	エンコードアドレスのアドレスファミリーは 2(IPv6)，エンコードタイプは 0 固定。IPv6 以外の PIM-SM とは接続できない。
	RFC には PIM メッセージのヘッダに PIM バージョンを設定するフィールドがある。	PIM バージョンは 2 固定。 PIM バージョン 1 と接続できない。
Join/Prune フラグメント	Join/Prune メッセージはネットワークの MTU を超えてもフラグメントできる。	送信する Join/Prune メッセージのサイズが大きい場合，8k バイトに分割して送信する。さらに分割して送信する Join/Prune メッセージはネットワークの MTU 長で IP フラグメントによって送信される。
PMBR との接続	RFC では PMBR(PIM Border Router) との接続および (*，*，RP) エントリに関する仕様が記述されている。	PMBR との接続はサポートしていない。また，(*，*，RP) エントリもサポートしていない。
最短経路への切り替え	最短経路への切り替えタイミングの例としてデータレートを基に切り替える方法がある。	last-hop-router で最初のデータを受信したら，データレートをチェックしないで最短経路へ切り替える。

RFC		本装置
C-RP-Adv 受信と Bootstrap 送信	Bootstrap メッセージは生成したメッセージ長が最大パケット長を超えた場合にフラグメントすることが許される。しかし，フラグメント発生を抑止するためにランデブーポイント候補の最大数を定義することが望ましい。	ランデブーポイントで定義できるグループプレフィックスは最大 128 個である。 本装置では送信する Bootstrap メッセージのサイズが大きい場合，ネットワークの MTU 長で IP フラグメントして送信される。
Hello メッセージオプション	RFC では HoldTime オプション (タイプ 1) が定義されている。	HoldTime オプションのほかに，隣接ルータアドレスリストオプション (タイプ 24 およびタイプ 65001) を使用する。(「19.4.2　近隣検出」参照)

19.4.8　IPv6 PIM-SSM

PIM-SSM は PIM-SM の拡張機能です。PIM-SM と PIM-SSM は同時動作できます。PIM-SSM が使用するマルチキャストアドレスは IANA で割り当てられています。本装置では，コンフィグレーションで PIM-SSM が動作するマルチキャストアドレス (グループアドレス) のアドレス範囲を指定できます。指定したアドレス以外では PIM-SM が動作します。

PIM-SM はマルチキャストエントリ作成にマルチキャスト中継パケットが必要なのに対し，PIM-SSM はマルチキャスト経路情報 (PIM-Join) の交換で IPv6 マルチキャスト中継エントリを作成し，該当エントリでマルチキャストパケットを中継します。また，PIM-SSM ではランデブーポイントおよびブートストラップルータは必要ありません。したがって，マルチキャストパケットを中継するときのパケットのカプセル化およびカプセル化の解除がなくなり，効率の良いマルチキャスト中継が実現できます。PIM-SSM は MLDv2（INCLUDE モード）のホストと接続している場合に動作します。また，本装置では MLDv1 または MLDv2（EXCLUDE モード）のホストから PIM-SSM を利用できるようにする手段を提供します。

（1） IPv6 PIM-SSM メッセージサポート仕様

PIM-SM メッセージと同じです。

（2） IPv6 PIM-SSM を動作させる前提条件

本装置ではコンフィグレーションで次の設定が必要です。

- 各装置の設定
  PIM-SSM が動作するグループアドレスの範囲を設定します。
- MLDv2（INCLUDE モード）が動作するホストが直結している装置
  接続するインタフェースに MLDv2 を設定します。
- MLDv1 または MLDv2（EXCLUDE モード）が動作するホストが直結している装置
  接続するインタフェースに MLDv1 または MLDv2 を設定します。
  使用するグループアドレスに送信元アドレスを設定します。

（3） IPv6 PIM-SSM 動作（ホストが MLDv2（INCLUDE モード）の場合）

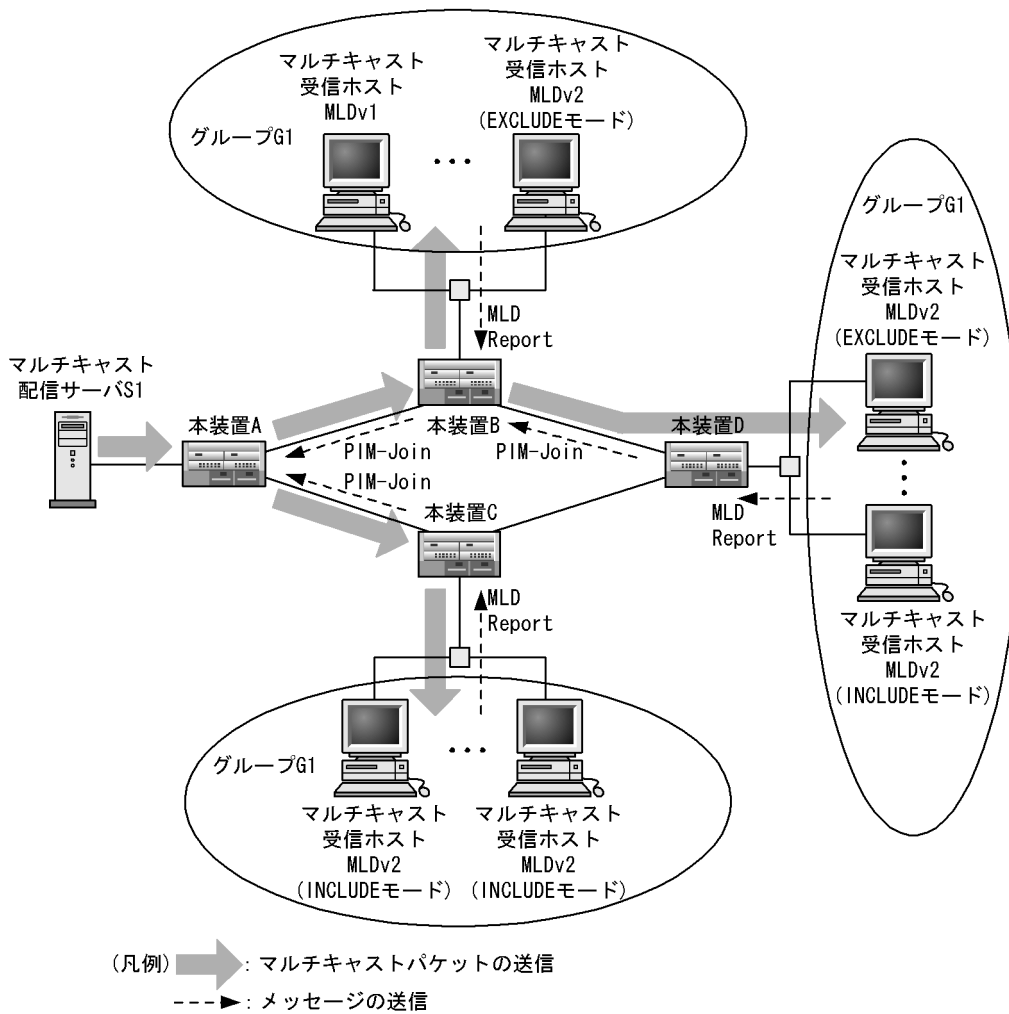
マルチキャストパケット配信サーバ (送信元アドレス：S1) がグループ 1(グループアドレス：G1) にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（MLDv2（INCLUDE モード））を受信します。
2. 参加要求（MLDv2（INCLUDE モード））を受信した装置は通知されたグループアドレス (G1) と送信

元アドレス (S1) から送信元アドレス (S1) の方向（ユニキャストのルーティング情報で決定）に PIM-Join を送信します。この場合，PIM-Join には，送信元アドレス (S1) とグループアドレス (G1) の情報が入ります。PIM-Join を受信した各装置は送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した装置は送信元アドレス (S1) とグループアドレス (G1) の IPv6 マルチキャスト経路情報を学習します。

3. マルチキャストパケット配信サーバ (S1) がグループ 1(G1) 宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習した IPv6 マルチキャスト経路情報から生成した IPv6 マルチキャスト中継エントリに従いパケットを中継します。

IPv6 PIM-SSM の動作概要を次の図に示します。

図 19-17　IPv6 PIM-SSM の動作概要

(4) IPv6 PIM-SSM 動作（ホストが MLDv1 または MLDv2（EXCLUDE モード）の場合）

マルチキャストパケット配信サーバ (送信元アドレス：S1) がグループ 1(グループアドレス：G1) にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（MLDv1 または MLDv2（EXCLUDE モード））を受信します。

2. 参加要求（MLDv1 または MLDv2（EXCLUDE モード））を受信した装置は通知されたグループアドレス (G1) とコンフィグレーションで定義したグループアドレスを比較します。グループアドレスが一致した場合，コンフィグレーションで定義した送信元アドレス (S1) の方向（ユニキャストのルーティング情報で決定）に PIM-Join を送信します。この場合，PIM-Join には，送信元アドレス (S1) とグループアドレス (G1) の情報が入ります。PIM-Join を受信した各装置は送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した装置は送信元アドレス (S1) とグループアドレス (G1) の IPv6 マルチキャスト経路情報を学習します。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(G1) 宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習した IPv6 マルチキャスト経路情報から生成した IPv6 マルチキャスト中継エントリに従いパケットを中継します。

IPv6 PIM-SSM の動作概要については，「図 19-17　IPv6 PIM-SSM の動作概要」を参照してください。

（5） 近隣検出

PIM-SM(「19.4.2　近隣検出」) と同じです。

（6） Forwarder の決定

PIM-SM(「19.4.3　Forwarder の決定」) と同じです。

（7） DR の決定および動作

PIM-SM(「19.4.4　DR の決定および動作」) と同じです。

（8） 冗長経路時の注意事項

PIM-SM(「19.4.5　冗長経路時の注意事項」) と同じです。

19.4.9　MLDv2 使用時の IPv6 経路制御動作

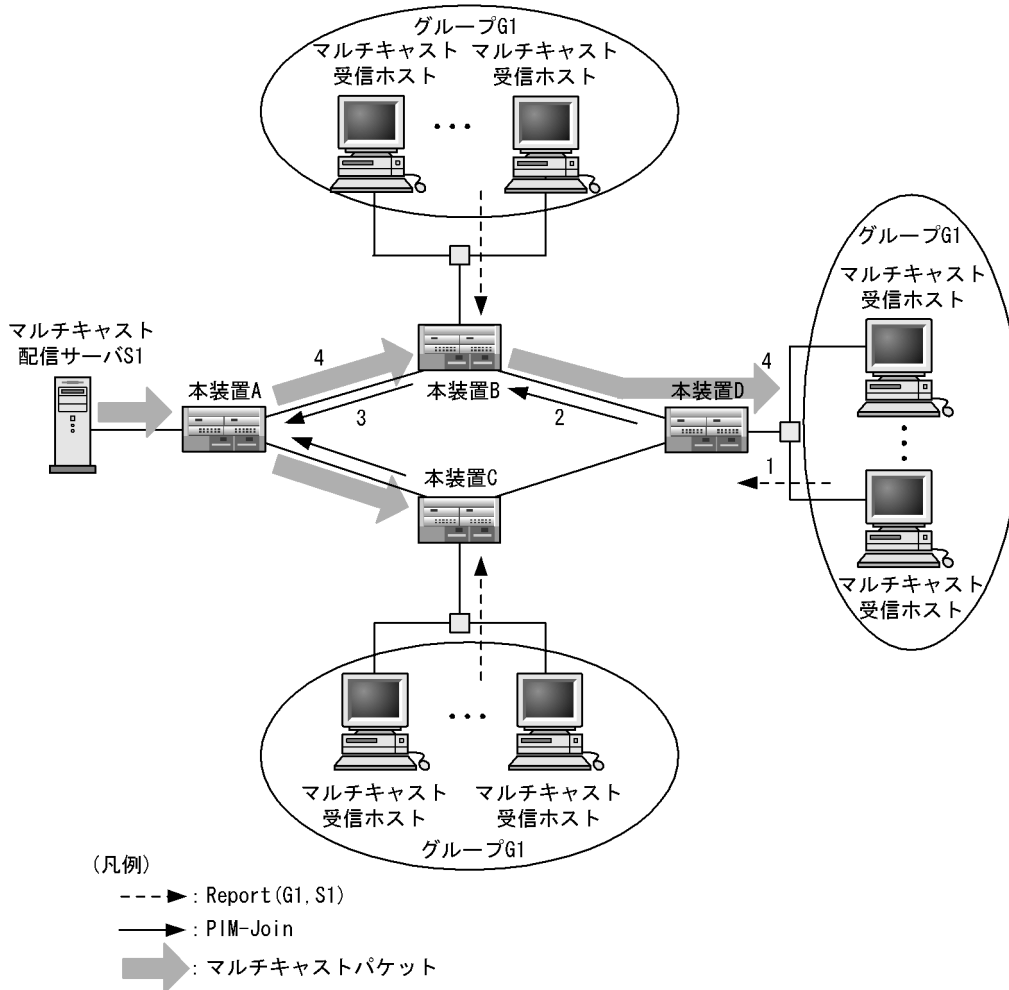
（1） MLDv2 使用時の IPv6 PIM-SSM 動作

PIM-SSM を使用するためには送信元の情報が必要となります。本装置では MLDv1 を使用する際には送信元をコンフィグレーションで設定することで PIM-SSM を使用することができます。MLDv2 では送信元をコンフィグレーションで設定することなく PIM-SSM を使用できます (コンフィグレーションで PIM-SSM を設定する必要があります)。

マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv6 PIM-SSM 動作を次に示します。

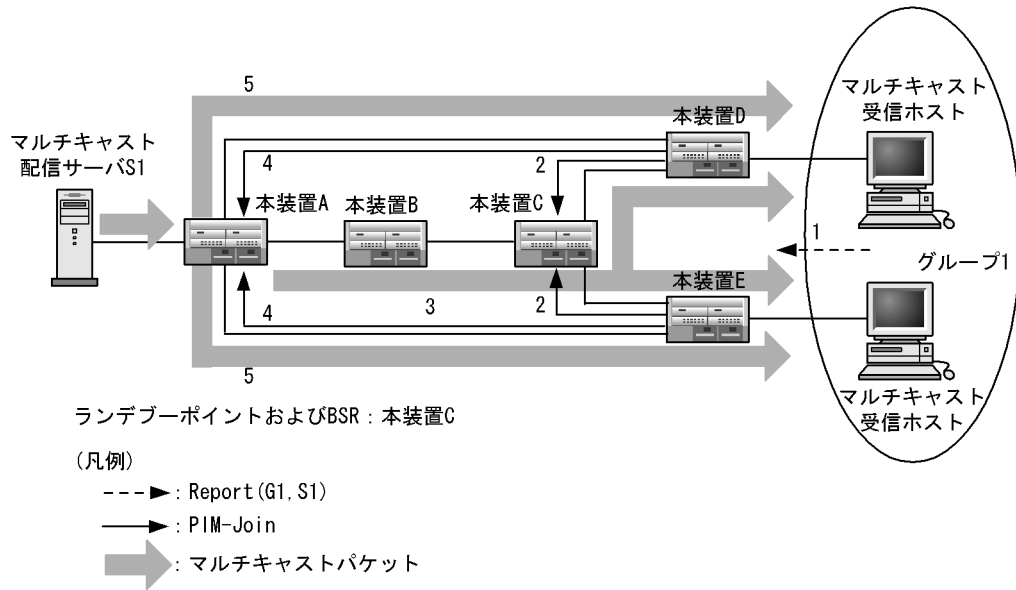
1. ホストからマルチキャストグループに参加するための MLDv2 Report(G1,S1) を受信します。
2. MLDv2 Report(G1,S1) を受信した装置は Report で通知されたグループアドレス (G1) とソースアドレス (S1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信した各装置は，送信元アドレス (S1) の方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した各装置は，PIM-Join を受信したインタフェースだけに送信元アドレス S1 からのマルチキャストパケットを中継するように (S1,G1) の配送ツリーを形成します。
4. マルチキャスト配信サーバ S1 がグループ G1 宛に送信したマルチキャストパケットを受信した装置はマルチキャスト中継情報に従いマルチキャストパケットを中継します。

図 19-18　MLDv2 使用時の IPv6 PIM-SSM 動作概要

(凡例)
- - -►：Report(G1,S1)
——►：PIM-Join
⇨：マルチキャストパケット

(2) MLDv2 使用時の IPv6 PIM-SM 動作

コンフィグレーションで PIM-SSM が設定されていない場合は PIM-SM で動作します。マルチキャスト配信サーバ (送信元アドレス S1) がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv6 PIM-SM 動作を次に示します。

1. ホストからマルチキャストグループに参加するための MLDv2 Report(G1,S1) を受信します。
2. MLDv2 Report(G1,S1) を受信した装置はランデブーポイントの方向にグループアドレス (G1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信したランデブーポイントは各グループの存在を認識します。マルチキャストパケットを送信元ネットワークからランデブーポイント経由で各グループメンバに配送するために，送信元を頂点としたランデブーポイント経由の配送ツリーを形成します。
4. 送信元から各グループメンバに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信元からの最短パスを決定します (PIM-Join を送信元の方向に送信し，最短パス配送ツリーを形成します)。
5. マルチキャスト配信サーバ S1 がグループ G1 宛に送信したマルチキャストパケットを受信した装置は最短パス配送ツリーに従いマルチキャストパケットを中継します。

図 19-19　MLDv2 使用時の IPv6 PIM-SM 動作概要

（3） MLDv1/MLDv2 ホスト混在時の IPv6 経路制御

MLDv1 で PIM-SSM を使用する設定をしている状態で，MLDv1 と MLDv2 ホストが混在する場合の IPv6 経路制御動作について説明します。

コンフィグレーションで設定した PIM-SSM 対象アドレス範囲に含まれるグループアドレスに対して加入要求を受けた場合は，次の表に示すように PIM-SSM が動作します。MLDv1 Report で加入要求を受けた場合，送信元リストはコンフィグレーションで設定した送信元アドレスを使用します。MLDv1 Report と MLDv2 Report で同じグループアドレスに対して加入要求を受けた場合，送信元リストはコンフィグレーションで設定された送信元アドレスと MLDv2 Report に含まれる送信元リストを合わせたリストを使用します。

表 19-12　MLDv1/MLDv2 ホスト混在時の IPv6 経路制御動作

加入グループアドレス	MLDv1 Report※	MLDv2 Report
SSM アドレス範囲内	PIM-SSM	PIM-SSM
SSM アドレス範囲外	PIM-SM	PIM-SM

注※　MLDv1 ホストが送信する Report のグループアドレスに対してだけ MLDv1 グループメンバを登録します。

19.5　IPv6 マルチキャストソフト処理パケット制御機能

IPv6 マルチキャストソフト処理パケット制御機能とは，本装置が受信するマルチキャストデータパケットを，コンフィグレーションで設定した受信要因と受信パケット数に従って，制御することによって，マルチキャストパケット受信による本装置の輻輳を抑止する機能です。なお，当機能は中継パケットには影響ありません。

19.5.1　パケット制御対象受信要因

パケット制御の対象受信要因とその内容を次の表に示します。

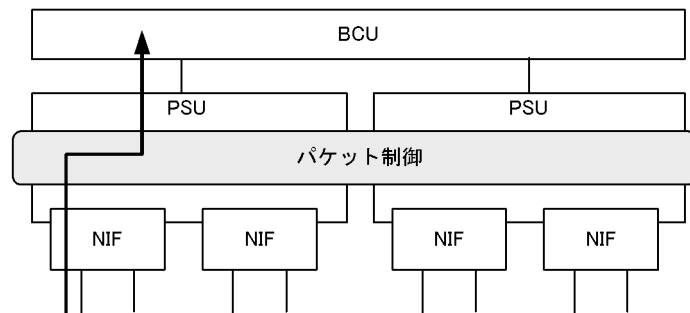
表 19-13　パケット制御対象受信要因

パケット受信要因	内容
wrong-incoming-interface	ハードウェアの IPv6 マルチキャスト中継エントリに登録済みのエントリと一致したマルチキャストデータパケットを別のインタフェースから受信した場合に発生する要因
cache-misshit	ハードウェアの IPv6 マルチキャスト中継エントリに存在しないマルチキャストデータパケットを受信した場合に発生する要因

19.5.2　パケット制御【SB-7800S】

（1）パケット制御概略

パケット制御の概略を次の図に示します。

図 19-20　パケット制御概略図

ネットワークインタフェースモジュール (NIF) から受信したソフト処理用データパケットを基本制御モジュール (BCU) に転送する際に，コンフィグレーションによって設定した受信要因と比較し，一致した場合，定義した受信パケット数に従って転送数を制御します。

（2）パケット制御実行単位

パケット制御を実行する単位は PSU 内蔵型高密度ポート NIF を除き，NIF 単位です。PSU 内蔵型高密度ポート NIF はポート単位にパケット制御を実行します。以下に詳細内容を示します。

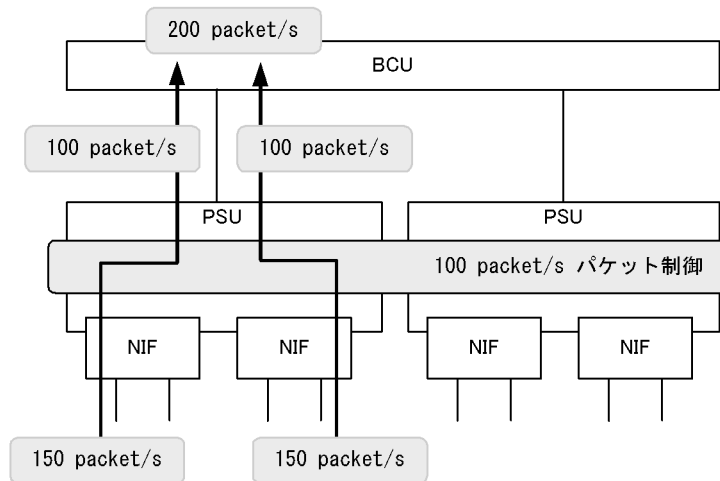
表 19-14　PSU 内蔵型高密度ポート NIF パケット制御実行単位

NIF	パケット制御実行単位				
S12-1G48S	右記ポート No. 単位	0 ～ 11	12 ～ 23	24 ～ 35	36 ～ 47

NIF	パケット制御実行単位				
S12-1G48T					
S22-10G4RX		0	1	2	3
S33-10G4RX					

(3) パケット制御例

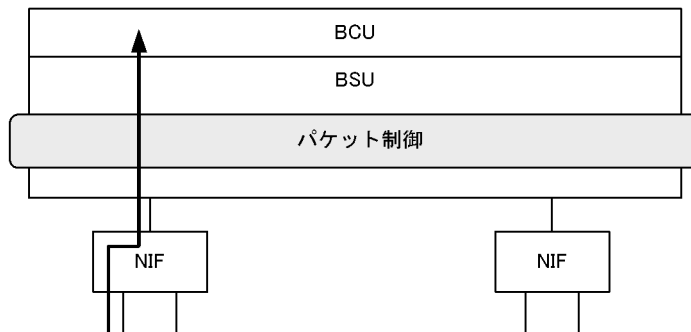
パケット制御例を次の図に示します。

図 19-21 パケット制御例

- コンフィグレーションによって,「100 packet/s」でパケット制御実行を指示
- 異なる NIF の 2 インタフェースから 150 packet/s でソフト処理用パケットを受信する
- NIF 単位にパケット制御が実行され,BCU には 200 packet/s でパケットが転送される

19.5.3 パケット制御【SB-5400S】

(1) パケット制御概略

パケット制御の概略を次の図に示します。

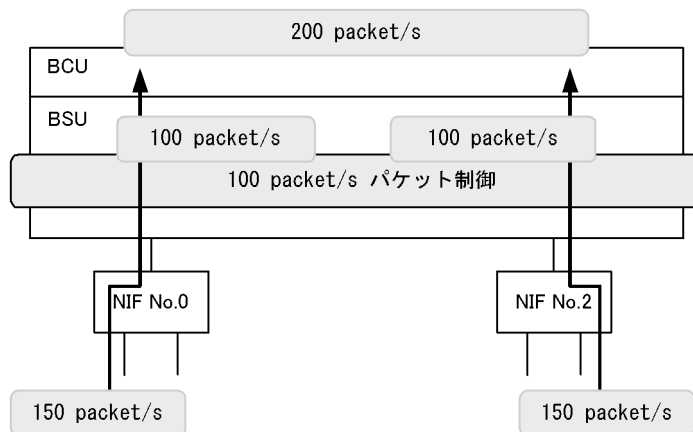
図 19-22 パケット制御概略図

ネットワークインタフェースモジュール (NIF) から受信したソフト処理用データパケットを基本制御モジュール (BCU) に転送する際に,コンフィグレーションによって設定した受信要因と比較し,一致した場合,定義した受信パケット数に従って転送数を制御します。

（2） パケット制御実行単位

パケット制御を実行する単位は NIF を搭載するスロット位置によって異なります。パケット制御はスロット位置 0 と 1，2 と 3 を制御単位として実行します。

（3） パケット制御例

パケット制御例を次の図に示します。

図 19-23　パケット制御例

- コンフィグレーションによって，「100 packet/s」でパケット制御実行を指示
- 異なる NIF(搭載スロット NO.0 と 2) の 2 インタフェースから 150 packet/s でソフト処理用パケットを受信する
- NIF を搭載するスロット位置が 0 と 2 のため各 NIF 単位にパケット制御が実行され，BCU には 200 packet/s でパケットが転送される

19.6 ネットワーク設計の考え方

19.6.1 IPv6 マルチキャスト中継

本装置で IPv6 マルチキャストパケットを中継する場合には次の点に注意してください。

（1） IPv6 PIM-SM および IPv6 PIM-SSM 共通

（a） 二重化装置での系切替に伴う中継断

本装置は，二重化装置による運用で現用系から待機系に切り替わる場合は，IPv6 マルチキャスト経路情報を再学習するまで IPv6 マルチキャスト通信が停止するので注意してください。

ただし，SB-7800S 使用時，IPv6 PIM-SSM の場合，コンフィグレーションによって，IPv6 マルチキャスト通信を停止することなく系切替ができます。

（b） ルーティングプログラムの再起動に伴う中継断

本装置は，restart ipv6-multicast コマンド実行による IPv6 マルチキャストルーティングプログラムの再起動を行う場合は，IPv6 マルチキャスト経路情報を再学習するまで IPv6 マルチキャスト通信が停止するので注意してください。

（c） ポイント - ポイント型の回線

ユニキャストのスタティック経路を設定したポイント - ポイント型の回線を使用して，IPv6 マルチキャスト通信を行う場合は，接続先アドレスを明示的に指定 (ゲートウェイ指定) してください。

（d） タイミングによるパケット追い越し

本装置で送信者からのマルチキャストデータと受信者側からの PIM-Join メッセージを同時に受信した場合，タイミングによっては一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります。

（2） IPv6 PIM-SM

IPv6 で PIM-SM を使用する場合は次の点に注意してください。

（a） ソフトウェア中継処理時のパケットロス

本装置は，最初の IPv6 マルチキャストパケット受信で IPv6 マルチキャスト通信を行うための IPv6 マルチキャスト中継エントリをハードウェアへ設定します。エントリを作成するまでの間ソフトウェアで IPv6 マルチキャストパケットを中継するため，一時的にパケットをロスする場合があります。

（b） ハードウェア中継切り替え時のパケット追い越し

本装置ではハードウェアへの IPv6 マルチキャスト中継エントリの設定が完了すると，それまでのソフトウェアによる IPv6 マルチキャストパケットの中継処理がハードウェア中継へと切り替わります。この時に一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります。

（c） パス切り替え時の二重中継またはパケットロス

本装置は，ランデブーポイント経由での IPv6 マルチキャストパケット中継時およびランデブーポイント経由から最短パス経由への切り替え時，一時的に二重中継またはパケットロスが発生する場合があります。

ランデブーポイント経由の IPv6 マルチキャストパケットの中継動作およびランデブーポイント経由から

最短パス経由切り替え動作は「19.4.1　IPv6 PIM-SM の動作」を参照してください。

(d) 装置アドレス定義必須

本装置を first-hop-router として使用する場合，ランデブーポイントへの通信には装置管理情報のローカルアドレスで定義された IPv6 アドレスが用いられます。そのため IPv6 PIM-SM では，IPv4 PIM-SM とは異なりランデブーポイントや BSR でない場合にも装置アドレスの定義が必須です。

(e) 装置アドレス到達可能性

本装置をランデブーポイントおよびブートストラップルータとして使用する場合，装置管理情報のローカルアドレスで定義された IPv6 アドレスがランデブーポイントとブートストラップルータのアドレスとなります。この装置管理情報のローカルアドレスは IPv6 マルチキャスト通信する全装置でユニキャストでのルート認識および通信ができる必要があります。

(f) 静的ランデブーポイント

静的ランデブーポイントは，BSR を使用しないでランデブーポイントを指定する機能です。静的ランデブーポイントはコンフィグレーションによって定義します。

静的ランデブーポイントは BSR から Bootstrap メッセージによって広告されたランデブーポイント候補との共存もできます。共存時，静的ランデブーポイントは BSR から Bootstrap メッセージによって広告されたランデブーポイント候補よりも優先されます。

なお，ランデブーポイント候補のルータは，ランデブーポイントルータアドレスが自アドレスであることを認識することでランデブーポイントとして動作します。したがって，BSR を使用しないで静的ランデブーポイントを使ってネットワークを設計する場合は，ランデブーポイント候補のルータでも静的ランデブーポイントの定義が必要です。

また，静的ランデブーポイントを使用する場合，同一ネットワーク上の全ルータに対して同じ定義をする必要があります。

(3) IPv6 PIM-SSM

IPv6 で PIM-SSM を使用する場合は次の点に注意してください。

(a) 系切替時の nonstop forwarding【SB-7800S】

IPv6 PIM-SSM に系切替時に通信を継続することが可能な nonstop forwarding 機能をサポートしています。本機能は，コンフィグレーションで nonstop-forwarding を設定した場合だけ有効になります。
nonstop forwarding 機能使用時の注意事項を次に示します。

1. 系切替後の IPv6 マルチキャストルーティングテーブルの再学習完了時間は約 420 秒です。再学習の開始と終了は運用ログメッセージとして出力します。運用ログメッセージの詳細については，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. 系切替後の IPv6 マルチキャストルーティングテーブルの再学習状況は，次に示す運用コマンドで確認できます。各コマンドの詳細については，マニュアル「運用コマンドレファレンス Vol.2」を参照してください。
   - show ipv6 mroute
   - show ipv6 mcache
   - show ipv6 pim mcache
3. 系切替後の IPv6 マルチキャストルーティングテーブルの再学習時間内の注意事項を次に示します。各注意事項は再学習完了後に解消されます。
   - 再学習中に IPv6 マルチキャストデータの二重中継が発生した場合，その解消に時間が掛かることが

あります。
- 再学習中に中継中の IPv6 マルチキャストエントリのインタフェースに障害が発生し，その後回復した場合，再学習に関係なく中継を再開することがあります。
- 再学習中に中継中の IPv6 マルチキャストエントリのインタフェースをコンフィグレーションまたはプロトコル処理によって削除した場合，中継が停止しないことがあります。
- 再学習中に中継中の IPv6 マルチキャストエントリの受信インタフェースが変更された場合，パケットロスが発生することがあります。
- 再学習中に閉塞状態の PSU/NIF を運用状態にした場合，運用状態のほかの PSU/NIF での IPv6 マルチキャスト中継が一時的に停止することがあります。
- 再学習中に閉塞状態の PSU/NIF を運用状態にした場合，該当する PSU/NIF での IPv6 マルチキャスト中継の開始に時間が掛かることがあります。これは，次に示す条件をすべて満たしているときに発生することがあります。
  ・IPv6 マルチキャストエントリの中継先インタフェースが VLAN またはリンクアグリゲーションである場合
  ・該当 VLAN またはリンクアグリゲーションが複数 PSU にわたっている場合
  ・該当 VLAN またはリンクアグリゲーションの閉塞状態である PSU/NIF を運用状態にした場合

4. nonstop forwarding が有効な状態で系切替したあと，マルチキャスト中継エントリを再学習している間，PIM-SSM の動作範囲をコンフィグレーションで変更しないでください。マルチキャスト中継エントリ再学習期間中に PIM-SSM 動作範囲をコンフィグレーションで変更し，マルチキャスト中継エントリが PIM-SM から PIM-SSM 経路または PIM-SSM から PIM-SM 経路となった場合，マルチキャスト中継の動作は保証できません。
5. 系切替時に IPv6 マルチキャストインタフェースの認識に時間が掛かる場合があります。pim6 コンフィグレーションの hello-interval がデフォルト値の場合，45 秒間 IPv6 マルチキャストインタフェースの認識ができないと近隣ルータがタイムアウトし，IPv6 マルチキャスト中継が中断します。その場合は，pim6 コンフィグレーションの hello-interval，join-prune-interval の値を大きくしてください。hello-interval，join-prune-interval の算出式と，IPv6 マルチキャストインタフェースを 2,000 個定義した場合の推奨値を次の表に示します。

表 19-15　hello-interval，join-prune-interval の算出式と，IPv6 マルチキャストインタフェースを 2,000 個定義した場合の推奨値

設定項目	算出式（秒）	マルチキャストインタフェースを 2,000 個定義した場合の推奨値（秒）
hello-interval	a ／ 1.5	30
join-prune-interval	（a + b + c + d + e）／ 2.5	140

a：装置切り替え時間
系切替後，運用コマンド show ipv6 pim interface または show ipv6 mld interface コマンドで全 IPv6 マルチキャストインタフェースが表示されるまでの時間に余裕を持たせた（約 5 割増）時間。

b：MLD Query メッセージ送信周期

c：Multicast Listner Report 最大応答待ち時間（10 秒固定）

d：近隣ルータからの PIM-Hello メッセージ最大受信周期

e：MLD Report/PIM Join メッセージ集中によるプロトコル処理時間（15 秒固定）

19.6.2　冗長経路 (回線障害などによる経路切り替え)

本装置で IPv6 マルチキャスト経路が冗長経路になっている場合，次の点に注意してください。

（1） IPv6 PIM-SM の使用

IPv6 PIM-SM の場合，次に示す経路切り替えで IPv6 マルチキャスト通信が再開するまで時間がかかるので注意してください。時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

- 優先経路が切り替わった場合，通信再開までには次に示す時間がかかる場合があります。

```
U+20秒
```

- 回線障害により優先経路から冗長経路が切り替わった場合，通信再開までには次に示す時間がかかる場合があります。

```
U<5の時:
5～10秒
U≧5の時:
U+0～50秒
```

- 回線復旧により冗長経路から優先経路に切り戻った場合，通信再開までには次に示す時間がかかる場合があります。

```
0～(送信者方向のHello送信周期+20)秒（デフォルトでは30+20=50秒）
```

- ランデブーポイントおよび BSR が他装置に切り替わった（障害やコンフィグレーションなどによってランデブーポイントおよび BSR を他装置にする）場合，通信再開までに最大 340 秒＋加入通知時間かかる場合があります。
- DR が他装置に切り替わった場合，通信再開までに最大 240 秒＋加入通知時間かかる場合があります。

障害による冗長経路切り替えだけでなく構成変更によって意識的に経路切り替えを行った場合も，IPv6 マルチキャスト通信がこれらの時間停止する場合があります。システムの構成変更は計画的に実施してください。

特にランデブーポイントおよび BSR を別装置に変更する場合は，新しいランデブーポイントおよび BSR のコンフィグレーションの priority 値を古いランデブーポイントおよび BSR の値よりも優先度が高くなるように設定してください。

（2） IPv6 PIM-SSM の使用

- 優先経路が切り替わった場合，通信再開までに次に示す時間がかかる場合があります。

```
U+20秒
```

- 回線障害により優先経路から冗長経路が切り替わった場合，通信再開までには次に示す時間がかかることがあります。

```
U<5の時:
5～10秒
U≧5の時:
U+0～135秒
```

- 回線復旧により冗長経路から優先経路に切り戻った場合，通信再開までには次に示す時間がかかることがあります。

```
0秒
```

ただし，切り戻りにかかる時間は次に示す時間がかかります。

U+0～(送信者方向のHello送信周期+20)秒（デフォルトでは30+20=50秒）

19.6.3 適応ネットワーク構成

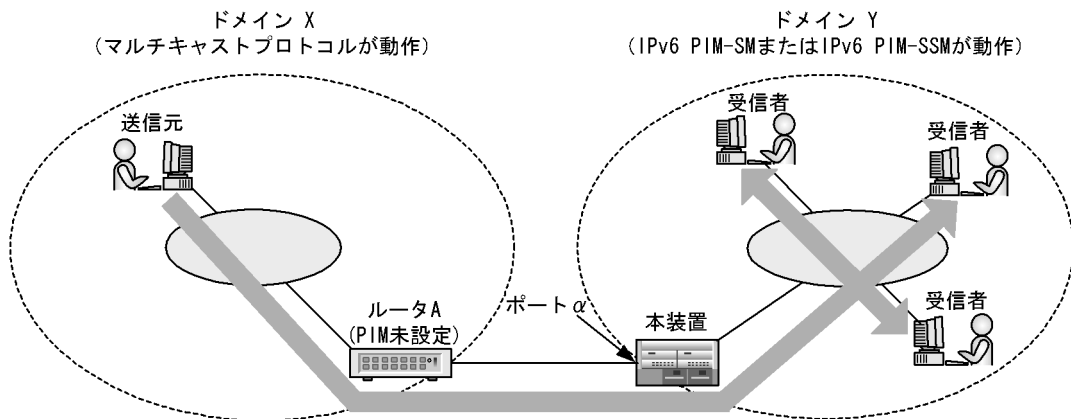
IPv6 マルチキャストはサーバ (送信者) から各グループ (受信者) にデータを配信する 1(送信者) : N(受信者) の片方向通信に適します。IPv6 マルチキャストの推奨ネットワーク構成，注意事項を次に示します。

（1） IPv6 PIM-SM および IPv6 PIM-SSM 共通

（a） 適用構成

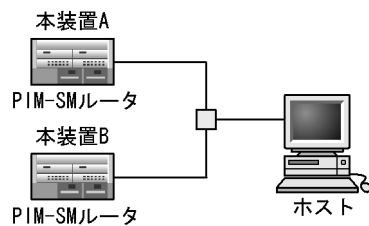
IPv6 PIM-SM または IPv6 PIM-SSM(以下，PIM と略す) では送信者から受信者に至る経路上のすべてのルータで PIM の設定が必要となります。このため，途中で PIM を設定していないルータがあると，マルチキャストパケットの中継が行えません。隣接ルータが PIM を設定していない場合には，上流ポートの指定を行うとパケットの中継ができるようになります。

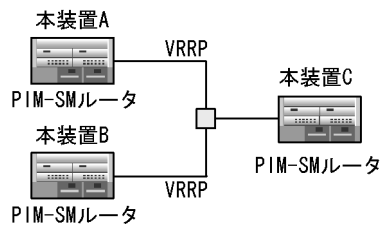
「図 19-24　IPv6 上流ポートを指定する場合の適応例」は上流ポートを指定する場合の適用例です。ルータ A と本装置は異なるマルチキャストドメインに属しているため，これらの間には PIM が設定されていません。一方，ドメイン X にいる送信元からドメイン Y にいる受信者にマルチキャストデータを送信したいという要求があります。ルータ A と本装置の間で PIM が動作していないので，送信者 S から送られたマルチキャストデータは本装置にて廃棄されます。ここで本装置のポート α に送信者 S への上流ポートを指定すると，ドメイン Y 内へのマルチキャストパケットの転送が行われるようになります。

図 19-24　IPv6 上流ポートを指定する場合の適応例

上流ポートの指定は上図のような構成に適用されますので，これ以外の構成ではマルチキャストパケットの中継ができなくなる可能性があります。

（b） 注意が必要な構成

次に示す構成で IPv6 PIM-SM または IPv6 PIM-SSM を使用する場合，注意が必要です。

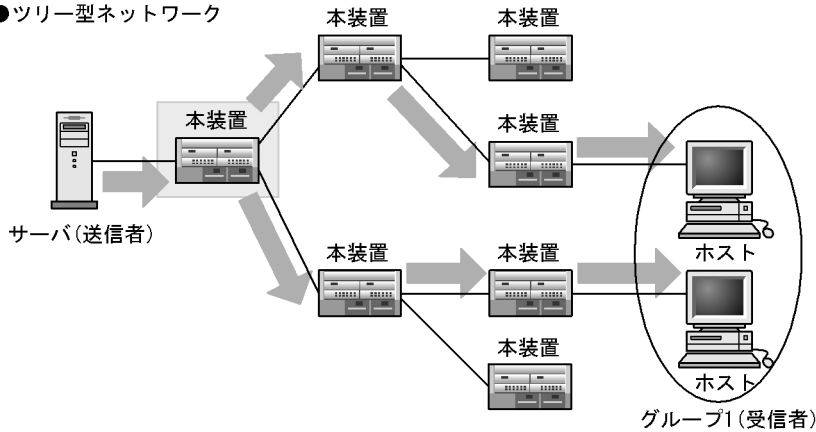
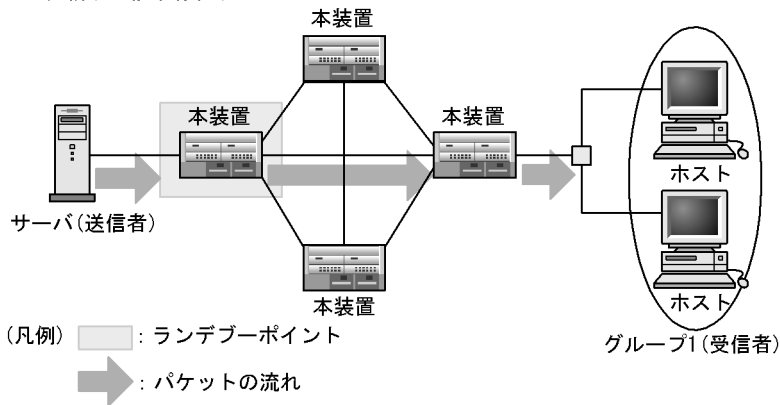
● 次の図に示す構成のようにホストと直接接続するルータが同一ネットワーク上に複数存在するインタフェースには，必ず PIM-SM を動作させてください。
同一ネットワーク上に複数のルータが存在するインタフェースに PIM-SM を動作させずに MLD だけを動作させた場合は，マルチキャストデータが二重中継される場合があります。

本装置A
PIM-SMルータ
本装置B
PIM-SMルータ
ホスト

● 次の図に示す構成のように本装置 C が本装置 A と本装置 B に VRRP を設定した仮想インタフェースをゲートウェイとするスタティックルートを設定した環境では，PIM プロトコルが上流ルータを検出できず，マルチキャスト通信ができません (PIM-SSM も同じです)。
この構成でマルチキャスト通信する場合は，本装置 C にランデブーポイントアドレスと BSR アドレスとマルチキャストデータ送信元アドレスへのゲートウェイアドレスを本装置 A または本装置 B の実アドレスとするスタティックルートを設定する必要があります。

(2)　IPv6 PIM-SM

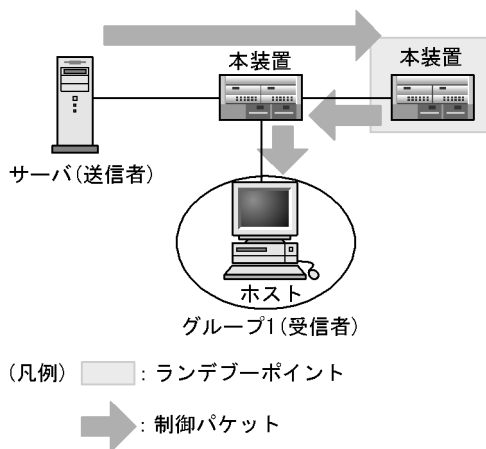
(a)　推奨構成

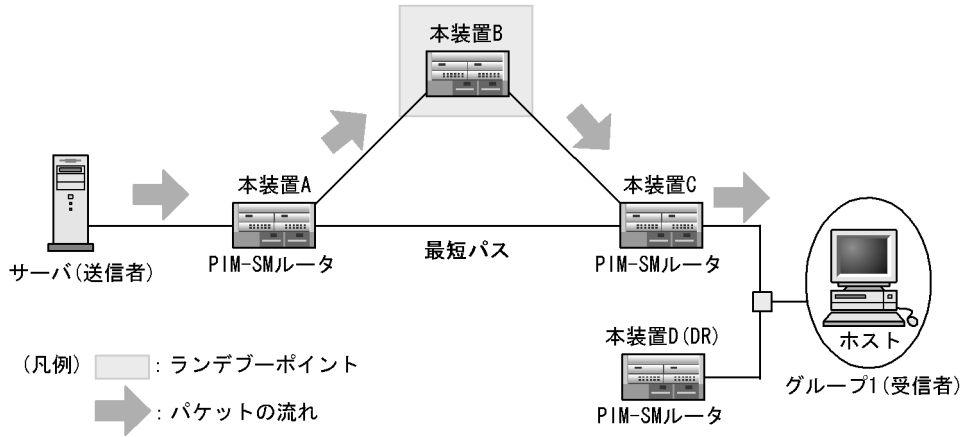
IPv6 PIM-SM によるネットワーク構成に当たっては，ツリー型ネットワーク構成および冗長経路が存在するネットワーク構成を推奨します。ただし，ランデブーポイントの配置には十分注意してください。ランデブーポイント経由の IPv6 マルチキャスト通信でのカプセル化処理および最短パス確立後のカプセル化抑止パケットの処理は，各ルータに負荷がかかるため，ランデブーポイントは送信者の直近に置くことをお勧めします。

IPv6 PIM-SM 推奨ネットワーク構成を次の図に示します。

図 19-25　IPv6 PIM-SM 推奨ネットワーク構成

(b)　不適応な構成

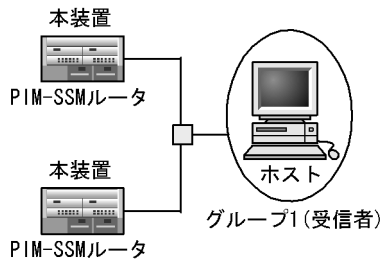
次に示す構成で IPv6 PIM-SM は使用しないでください。

● 送信者とランデブーポイントの間に受信者が存在する構成
次に示す構成でサーバからグループ 1 の IPv6 マルチキャスト通信を行う場合，ランデブーポイント経由の中継が効率よく行えません。

● DR である IPv6 PIM-SM ルータが IPv6 マルチキャストグループ (受信者) の存在する回線に対してだけ接続している構成

次に示す構成でグループ 1 宛ての IPv6 マルチキャスト通信をした場合，送信者とグループ 1 間で最短パスが確立しないことがあります。このため，ランデブーポイントを経由する IPv6 マルチキャスト通信が続くことになります。
この場合，DR である本装置 D はグループ 1 が存在する回線とは別の回線でランデブーポイントや送信者に至る経路を確保するようにネットワーク構築してください。

(3)　IPv6 PIM-SSM

(a)　注意が必要な構成

次に示す構成で IPv6 PIM-SSM を使用する場合注意が必要です。

● IPv6 マルチキャストグループ (受信者) と同一回線上に複数の IPv6 PIM-SSM ルータが動作する構成
次に示す構成で MLDv1 で PIM-SSM を動作させる場合は，同一回線上のすべてのルータをコンフィグレーションコマンド ssm(pim6 sparse モード) および ssm-join(mld モード) で設定してください。

(b)　端末側に複数のアドレスを設定したときの注意事項

SSM 通信時，データ送信を行う端末に複数の IPv6 アドレスを付与して運用する場合，送信されるデータの送信元アドレスが本装置に設定した ssm-join の送信元アドレス情報と一致するようにしてください。特に，RA などのアドレス自動設定機能を使用した場合は，端末側が自動設定されたアドレスを使用して通信を行う場合があります。

付録

付録 A　準拠規格

付録 A.1　イーサネット

表 A-1　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R **【SB-7800S】**, 10GBASE-W **【SB-7800S】**	ISO/IEC 8802.3 [ANSI/IEEE Std 802.3]	CSMA/CD Access Method and Physical Layer Specifications
	ISO 8802.2 [ANSI/IEEE Std 802.2]	Logical Link Control (LLC)
	IEEE 802.1Q	IEEE Standards for Local and Metropolitan Networks : Virtual Bridged local Area Networks ※
	IEEE Std 802.3x-1997	Specification for 802.3x Full Duplex Operation
	Ethernet V 2.0	The Ethernet-A Local Area Network:Data Link Layer and Physical Layer Specifications
	RFC 894	Standard for the Transmission of IP Datagrams over Ethernet Networks.
	RFC1042	Standard for the Transmission of IP Datagrams over IEEE802 Networks.
	RFC1398	Definitions of Managed Objects for the Ethernet-like Interface Types.
	RFC1757	Remote Network Monitoring Management Information Base.
	RFC2464	Transmission of IPv6 Packets over Ethernet Networks
10GBASE-R **【SB-7800S】**, 10GBASE-W **【SB-7800S】**	IEEE 802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10Gb/s Operation

注　1000BASE-LH の光インタフェースは標準化されていないため本装置の独自仕様です。

注※　GVRP/GMRP はサポートしていません。

表 A-2　リンクアグリゲーションの準拠規格

規格	名称
IEEE802.3ad (IEEE Std 802.3ad-2000)	Aggregation of Multiple Link Segments

付録 A.2　POS【SB-7800S】

表 A-3　POS の準拠規格

種別	規格	名称
OC-192c/STM-64 POS	ITU-T G.691(10/2000)	Optical interfaces for single channel STM-64, STM-256 systems and other SDH systems with optical amplifiers
	Bellcore GR-253-COREIssue 2 Revision 2	Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria
	RFC1332	The PPP Internet Protocol Control Protocol (IPCP)

種別	規格	名称
	RFC1377	The PPP OSI Network Layer Control Protocol (OSINLCP)
	RFC1661	The Point-to-Point Protocol (PPP)
	RFC1662	PPP in HDLC-like Framing
	RFC2472	IP Version 6 over PPP
	RFC2615	PPP over SONET/SDH
OC-48c/STM-16 POS	ITU-T G.957(06/99)	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
	ITU-T G.958(11/94)	Digital line systems based on the synchronous digital hierarchy for use on optical fiber cables
	Bellcore GR-253-COREIssue 2 Revision 2	Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria
	RFC1332	The PPP Internet Protocol Control Protocol (IPCP)
	RFC1377	The PPP OSI Network Layer Control Protocol (OSINLCP)
	RFC1661	The Point-to-Point Protocol (PPP)
	RFC1662	PPP in HDLC-like Framing
	RFC2472	IP Version 6 over PPP
	RFC2615	PPP over SONET/SDH

付録 A.3　レイヤ 2 スイッチ

表 A-4　VLAN の準拠規格および勧告

規格	名称
IEEE802.1Q (IEEE Std 802.1Q-1998)	Virtual Bridged Local Area Networks
IEEE802.1u (IEEE Std 802.1u-2001)	Virtual Bridged Local Area Networks - Amendment 1: Technical and editorial corrections
IEEE802.1v (IEEE Std 802.1v-2001)	Virtual Bridged Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port

表 A-5　スパニングツリーの準拠規格および勧告

規格	名称
IEEE802.1D (ANSI/IEEE Std 802.1D-1998 Edition)	Media Access Control (MAC) Bridges (The Spanning Tree Algorithm and Protocol)
IEEE802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration
IEEE802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

表 A-6　IGMP snooping/MLD snooping の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 A.4　IPv4 ネットワーク

表 A-7　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR):an Address Assignment and Aggregation Strategy
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC1933(1996 年 4 月)	Transition Mechanisms for IPv6 Hosts and Routers

表 A-8　DHCP/BOOTP リレーエージェントの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1542(1993 年 10 月)	Clarifications and Extensions for the Bootstrap Protocol
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC3046(2001 年 1 月)	DHCP Relay Agent Information Option

表 A-9　DHCP サーバ機能の準拠規格

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions
RFC2136(1997 年 4 月)	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC3679(2004 年 1 月)	Unused Dynamic Host Configuration Protocol (DHCP) Option Codes

表 A-10　DNS リレー機能の準拠規格

規格番号 (発行年月)	規格名
RFC1034(1987 年 3 月)	Domain names - concepts and facilities
RFC1035(1987 年 3 月)	Domain names - implementation and specification

付録 A.5　RIP/OSPF

表 A-11　RIP/OSPF の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1058(1988 年 6 月)	Routing Information Protocol
RFC2453(1998 年 11 月)	RIP Version 2
RFC2328(1998 年 4 月)	OSPF Version 2
RFC1587(1994 年 3 月)	The OSPF NSSA Option
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC2370(1998 年 7 月)	The OSPF Opaque LSA Option
RFC3623(2003 年 11 月)	Graceful OSPF Restart
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement

付録 A.6　BGP4【**OP-BGP**】

表 A-12　BGP4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-10.txt (2004 年 6 月)	Graceful Restart Mechanism for BGP

付録 A.7　IS-IS【**OP-ISIS**】

表 A-13　IS-IS の準拠規格および勧告

規格番号	規格名
ISO 9542:1988	Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)
ISO/IEC 10589:1992	Information technology - Telecommunications and information exchange between system - Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)
RFC1195(1990 年 12 月)	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

規格番号	規格名
RFC2763(2000 年 2 月)	Dynamic Hostname Exchange Mechanism for IS-IS
RFC2966(2000 年 10 月)	Domain-wide Prefix Distribution with Two-Level IS-IS
RFC3277(2002 年 4 月)	Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance
RFC3373(2002 年 9 月)	Three-Way Handshake for IS-IS Point-to-Point Adjacencies
RFC3567(2003 年 7 月)	Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC3784(2004 年 6 月)	Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC3847(2004 年 7 月)	Restart Signaling for Intermediate System to Intermediate System (IS-IS)
draft-ietf-isis-ipv6-06.txt (2005 年 10 月)	Routing IPv6 with IS-IS

付録 A.8　IPv4 マルチキャスト【OP-MLT】

表 A-14　IP マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2236	Internet Group Management Protocol,Version2
draft-ietf-idmr-dvmrp-v3-06.txt (1998 年 3 月)	Distance Vector Multicast Routing Protocol
draft-ietf-pim-v2-03.txt (1999 年 6 月)	Protocol Independent Multicast Version2 Dense Mode Specification
RFC2362	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification
draft-ietf-pim-sm-v2-new-05.txt (2002 年 3 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification (revised)
RFC3376	Internet Group Management Protocol, Version 3
RFC4601(2006 年 8 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification (revised)
draft-ietf-pim-sm-bsr-07.txt ※ 2	Bootstrap Router (BSR) Mechanism for PIM

注※ 1　この規格は PIM-SSM 関連部だけ準拠しています。

注※ 2　この規格は PIM-Hello オプションの Generation ID 関連部だけ準拠しています。

付録 A.9　IPv6 ネットワーク

表 A-15　IPv6 ネットワークの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2373(1998 年 7 月)	IP Version 6 Addressing Architecture
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2461(1998 年 12 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462(1998 年 12 月)	IPv6 Stateless Address Autoconfiguration
RFC2463(1998 年 12 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

規格番号 (発行年月)	規格名
RFC2473(1998 年 12 月)	Generic Packet Tunneling in IPv6 Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
RFC3056(2001 年 2 月)	Connectioin of IPv6 Domains via IPv4 Clouds
draft-ietf-ipv6-deprecate-rh0-01.txt (2007 年 6 月)	Deprecation of Type 0 Routing Headers in IPv6

表 A-16　IPv6 DHCP サーバ機能の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3315(2003 年 7 月)	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC3633(2003 年 12 月)	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC3646(2003 年 12 月)	DNS Configuration Options for DHCPv6
RFC4075(2005 年 3 月)	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
RFC3319(2003 年 7 月)	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC3736(2004 年 4 月)	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

付録 A.10　RIPng/OSPFv3

表 A-17　RIPng/OSPFv3 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2080(1997 年 1 月)	RIPng for IPv6
RFC2740(1999 年 12 月)	OSPF for IPv6
RFC3623(2003 年 11 月)	Graceful OSPF Restart
draft-kompella-ospf-opaquev2-00.txt (2002 年 10 月)	OSPFv2 Opaque LSAs in OSPFv3
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement

付録 A.11　BGP4+【**OP-BGP**】

表 A-18　BGP4+ の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2545(1999 年 3 月)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC2858(2000 年 6 月)	Multiprotocol Extensions for BGP-4
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4

規格番号 (発行年月)	規格名
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-10.txt (2004 年 6 月)	Graceful Restart Mechanism for BGP

付録 A.12　IPv6 マルチキャスト【OP-MLT】

表 A-19　IPv6 マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2710(1999 年 10 月)	Multicast Listener Discovery (MLD) for IPv6
RFC2362(1998 年 6 月)	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification
draft-ietf-pim-sm-v2-new-03.txt (2001 年 7 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
draft-ietf-pim-sm-v2-new-05.txt (2002 年 3 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
RFC3810(2004 年 6 月)	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC4601(2006 年 8 月) ※ 3	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
draft-ietf-pim-pim-sm-bsr-07.txt ※ 3	Bootstrap Router (BSR) Mechanism for PIM

注※ 1　この規格は IPv6 関連部だけ準拠しています。
注※ 2　この規格は PIM-SSM だけ準拠しています。
注※ 3　この規格は PIM-Hello オプションの Generation ID 関連部だけ準拠しています。

付録 A.13　Diff-serv

表 A-20　Diff-serv の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC2475(1998 年 12 月)	An Architecture for Differentiated Services
RFC2597(1999 年 6 月)	Assured Forwarding PHB Group
RFC2598(1999 年 6 月)	An Expedited Forwarding PHB

付録 A.14　IEEE802.1X

表 A-21　IEEE802.1X の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1X(2001 年 6 月)	Port-Based Network Access Control
RFC2284(1998 年 3 月)	PPP Extensible Authentication Protocol (EAP)
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)

規格番号 (発行年月)	規格名
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC2869(2000 年 6 月)	RADIUS Extensions
RFC3579(2003 年 9 月)	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC3580(2003 年 9 月)	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

付録 A.15　VRRP

表 A-22　VRRP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2338(1998 年 4 月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-ipv6-spec-02.txt (2002 年 2 月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-ipv6-spec-07.txt (2004 年 10 月)	Virtual Router Redundancy Protocol for IPv6
RFC3768(2004 年 4 月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-unified-mib-04.txt (2006 年 9 月)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6

付録 A.16　IEEE802.3ah/UDLD

表 A-23　IEEE802.3ah/UDLD の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.3ah(2004 年 9 月)	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

付録 A.17　SNMP

表 A-24　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1354(1992 年 7 月)	IP Forwarding Table MIB
RFC1471(1993 年 6 月)	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC1473(1993 年 6 月)	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC1474(1993 年 6 月)	The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol

規格番号 (発行年月)	規格名
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657(1994 年 7 月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC1659(1994 年 7 月)	Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC1850(1995 年 11 月)	OSPF Version2 Management Information Base
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2115(1997 年 9 月)	Management Information Base for Frame Relay DTEs Using SMIv2
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2452(1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC2454(1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC2465(1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC2466(1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2495(1999 年 1 月)	Definitions of Managed Objects for the DS1,E1,DS2 and E2 Interface Types
RFC2496(1999 年 1 月)	Definitions of Managed Objects for the DS3/E3 Interface Type
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC2787(2000 年 3 月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2932(2000 年 10 月)	IPv4 Multicast Routing MIB
RFC2933(2000 年 10 月)	Internet Group Management Protocol MIB
RFC2934(2000 年 10 月)	Protocol independent Multicast MIB for IPv4
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework

規格番号 (発行年月)	規格名
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet- standard Network Management Framework

付録 A.18　sFlow

表 A-25　sFlow の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3176(2001 年 9 月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.19　NetFlow【OP-ADV】

表 A-26　NetFlow の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3954(2004 年 10 月)	Cisco Systems NetFlow Services Export Version 9

付録 A.20　LLDP

表 A-27　LLDP の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1AB/D6.0(2003 年 10 月)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery

付録 A.21　RADIUS/TACACS+

表 A-28　RADIUS/TACACS+ の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)

規格番号 (発行年月)	規格名
RFC2866(2000 年 6 月)	RADIUS Accounting
draft-grant-tacacs-02.txt (1997 年 1 月)	The TACACS+ Protocol Version 1.78

付録 A.22　SYSLOG

表 A-29　SYSLOG の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol

付録 A.23　NTP

表 A-30　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC1305(1992 年 3 月)	Network Time Protocol (Version 3)

付録 B　謝辞 (Acknowledgments)

[GateD]

Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.
GateD Release 9.3.3

[SNMP]

software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.
****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.
****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.
****

* Primary Author:
Steve Waldbusser

* Additional Contributors:
Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/ 1995.
David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[BSDI Internet Server]

BERKELEY SOFTWARE DESIGN, INC.

Copyright (C) 1992, 1993, 1994, 1995, 1996, 1997 Berkeley Software Design, Inc.
This product includes BSDI Internet Server developed by Berkeley Software Design, Inc.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is

copyrighted by The Regents of the University of California.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

Contributors
- Sun Microsystems, Inc.
- Keith Muller
- Mark Nudelman
- Jan-Simon Pendry

AT&T (DAVID M. GAY)

Copyright (C) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

INFO-ZIP GROUP

This product includes Info-ZIP's software which is used for a part of the boot program. Info-ZIP's software (ZIP, UnZip and related utilities) is free and can be obtained as source code or executables from various bulletin board services and anonymous-ftp sites, including CompuServe's IBMPRO forum and ftp.uu.net:/pub/archiving/zip/*.

INTERNET SYSTEMS CONSORTIUM

Copyright (C) 2004 by Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SIGMASOFT, TH. LOCKERT

Copyright (C) 1994 SigmaSoft, Th. Lockert <tholo@sigmasoft.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SUN MICROSYSTEMS, INC.

Copyright (C) 1984, 1985, 1986, 1987, 1988, 1993 Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

UNIVERSITY OF TORONTO

Copyright (C) 1986 by University of Toronto.
Written by Henry Spencer. Not derived from licensed software.

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely,
subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

WASHINGTON UNIVERSITY IN SAINT LOUIS

WILDBOAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WILDBOAR PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MARTIN BIRGMEIER

Copyright (C) 1993 Martin Birgmeier
All rights reserved.

You may redistribute unmodified or modified versions of this source code provided that the above copyright notice and this and the following conditions are retained.

This software is provided "as is", and comes with no warranties of any kind. I shall in no event be liable for anything that happens to anyone/anything when using this software.

CHRISTOPHER G. DEMETRIOU

Copyright (C) 1993, 1994 Christopher G. Demetriou
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Christopher G. Demetriou.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DAVID HOVEMEYER

Copyright (C) 1995 David Hovemeyer <daveho@infocom.com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE DEVELOPERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE DEVELOPERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FRANK VAN DER LINDEN

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed for the NetBSD Project by Frank van der Linden
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THEO DE RAADT

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HENRY SPENCER

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.
This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

[diff, grep]

Copyright (C) 1988, 1989, 1992, 1993, 1994 Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

[less]

[tcpd]

[tcpdump]

[libpcap]

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[traceroute]

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: "This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors." Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[zlib]

Copyright notice:

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly   Mark Adler

gzip@prep.ai.mit.edu　madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

[Apache HTTP server]

[Xntp Program]

suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[MD5 Program]

Adapted from the RSA Data Security, Inc.
MD5 Message-Digest Algorithm.

[pimdd]

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd. The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted. The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[mrouted]

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and

modify the computer software "mrouted" (hereinafter called the "Program"), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.

2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied "as is," without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.

3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found
in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.

4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.

5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.

6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in a court in the State of California.

7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of ``Stanford''.

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[PIM sparse-mode pimd]

Copyright (C) 1998 by the University of Southern California.
All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute. The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

[LTCS (Label Traffic Control System)]

[KAME IPv6 STACK]

[CRUNCH]

[RADIUS]

[totd]

WIDE

University of Tromso

Invenia Innovation A.S.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993
The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and

the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libfetch]

Copyright (C) 1998 Dag-Erling Coïdan Smørgrav

All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer in this position and unchanged.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission
THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[iides]

Internet Initiative Japan Inc.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution with functional modification must include prominent notice stating how and when and by whom it is modified.
3. Redistributions in binary form have to be along with the source code or documentation which include above copyright notice, this list of conditions and the following disclaimer.
4. All commercial advertising materials mentioning features or use of this software must display the following acknowledgement:
 This product includes software developed by Internet Initiative Japan Inc.

THIS SOFTWARE IS PROVIDED BY ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

[Net-SNMP]

CMU/UCD

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Networks Associates Technology, Inc

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Cambridge Broadband Ltd.

Sun Microsystems, Inc.

Sparta, Inc

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

付録 C　用語解説

（英字）

ARP（Address Resolution Protocol）

IPv4 ネットワークで使用する通信プロトコルです。

AS（Autonomous System）

単一の管理権限で運用している独立したネットワークシステムのことを指します。

AS 境界ルータ

OSPF を使用して，AS 外経路を OSPF 内に導入するルータです。

BGP4（Border Gateway Protocol - version 4）

IPv4 ネットワークで使用する経路制御プロトコルです。

BGP4+（Multiprotocol Extensions for Border Gateway Protocol - version 4）

IPv6 ネットワークで使用する経路制御プロトコルです。

BGP4+ スピーカ

BGP4+ が動作するルータのことです。

BGP スピーカ

BGP が動作するルータのことです。

BPDU（Bridge Protocol Data Unit）

ブリッジ間でやり取りされるフレームです。

BSU（Basic packet Switching module）

ルーティング・QoS テーブル検索エンジンおよびパケット送信エンジンを持ち，ハードウェアでルーティングテーブル，フィルタリング・テーブルおよび QoS テーブルを検索し，パケットの送受信を行います。これによって高速な処理を実現しています。

CP 輻輳制御

BCU 内の CP で行う輻輳制御方式のことです。

自装置宛のフレームの輻輳を検知すると，その要因のフレームの受信を止めます。この制御の繰り返しによって，正常に動作している VLAN を収容しているポートの自宛通信への影響を抑えられます。

DHCP（Dynamic Host Configuration Protocol）

ネットワーク接続時に IP アドレスを自動設定するプロトコルです。リレーエージェント機能，サーバ機能およびクライアント機能があります。

DHCP/BOOTP リレーエージェント機能

DHCP/BOOTP サーバと DHCP/BOOTP クライアントが異なるサブネットにあるとき，コンフィグレーションで設定したサーバの IP アドレスを DHCP/BOOTP パケットの宛先 IP アドレスに設定して，パケットをサブネット間中継する機能です。

DHCP サーバ機能

IPv4 DHCP クライアントに対して，IP アドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

Diff-serv（Differentiated services）機能

IP パケットのヘッダ情報から優先度を決定して，その優先度に従ってルータが処理する機能です。

DNS リレー

DNS(Domain Name System) システムの異なるサブネットワークに存在するサーバとクライアント間で，クライアントからのパケットをドメインネームサーバのアドレスに中継する機能です。

DSCP（Differentiated Services Code Point）

IP フローの IP ヘッダ内 DS Field の上位 6 ビットです。

DS ドメイン

Diff-serv 機能を提供するネットワークです。

DVMRP（Distance Vector Multicast Routing Protocol）

IPv4 マルチキャストで使用する距離ベクトル型の経路制御プロトコルです。

EAP（Extensible Authentication Protocol）

拡張可能な認証プロトコル。具体的なセキュリティー機能を持たないため，EAP の中で使用される各種の認証プロトコルが実際のセキュリティー機能を提供します。

EAPOL（EAP Over LAN）

LAN 上で動作する拡張可能な認証プロトコル。IEEE802.1X に規定されている EAP のメッセージを LAN 上で伝送するための仕組みです。

EFM（Ethernet in the First Mile）

IEEE802.3ah 規格のことです。

FDB（Filtering Data Base）

トランスペアレント・ブリッジで使用されるテーブルです。FDB にはフレームの送信元 MAC アドレス，フレームを受信したポートおよび監視時刻が記録されます。

GSRP（Gigabit Switch Redundancy Protocol）

GSRP はレイヤ 2 のネットワークで，スイッチに障害が発生した場合でも，同一ネットワーク上の別スイッチを経由して通信経路を確保することを目的としたレイヤ 2 での装置の冗長化を実現する機能です。

ICMP（Internet Control Message Protocol）

IPv4 ネットワークで使用する通信プロトコルです。

ICMPv6（Internet Control Message Protocol version 6）

IPv6 ネットワークで使用する通信プロトコルです。

IGMP（Internet Group Management Protocol）

IPv4 ネットワークで使用するホスト - ルータ間のマルチキャストグループ管理プロトコルです。

IPv4（Internet Protocol version 4）

32 ビットの IP アドレスを持つインターネットプロトコルです。

IPv4 マルチキャスト

IPv4 マルチキャストは，ネットワーク内で選択されたグループに対して同一の情報を送信します。マルチキャストは送信者が受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷が軽減します。

IPv6（Internet Protocol version 6）

128 ビットの IP アドレスを持つインターネットプロトコルです。

IPv6 DHCP サーバ機能

IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの環境情報 (構成情報) を動的に割り当てるための機能です。

IPv6 グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスです。経路情報の集約を目的とした階層形式になっています。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを使用した通信に使用されます。

IPv6 サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスです。同一サイト内だけで有効なアドレスで，インターネットに接続されていないネットワークで自由に IPv6 アドレスを付ける場合に使用されます。

IPv6 マルチキャスト

IPv6 マルチキャストは IPv4 マルチキャストと同様の機能を IPv6 で実現します。

IPv6 リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80:: で，64 ビットのインタフェース ID 部を含むアドレスです。同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータがないときに使用されます。

IS-IS

IS-IS は，ルータ間の接続の状態から構成されるトポロジに基づき最短経路を計算するリンクステートプロトコルです。

LLDP（Link Layer Discovery Protocol）

隣接する装置情報を収集するプロトコルです。

MAC VLAN

送信元の MAC アドレス単位にグループ分けを行う VLAN です。

MIB（Management Information Base）

機器についての情報を表現するオブジェクトです。SNMP プロトコルで使用します。

MLD（Multicast Listener Discovery）

ルータ - ホスト間で使用される IPv6 マルチキャストグループ管理プロトコルです。

NAT（Network Address Translation）

ローカルネットワークのプライベートアドレスをインターネットなどで使用するグローバルアドレスに変換する機能です。

NDP（Neighbor Discovery Protocol）

IPv6 ネットワークで使用する通信プロトコルです。

NetFlow 統計

ネットワークを流れるトラフィックをサンプリングしてモニタし，モニタした NetFlow 統計情報を NetFlow コレクタと呼ばれる装置に集めて分析することによって，ネットワークの利用状況を把握する機能です。

NIF（Network Interface board）

接続する各メディアに対応したインタフェースを持つコンポーネントです。物理レイヤを処理します。

OADP（Octpower Auto Discovery Protocol）

OADP PDU（Protocol Data Unit）のやりとりによって隣接装置の情報を収集し，隣接装置の接続状況を表示する機能です。

OAM（Operations, Administration, and Maintenance）

ネットワークでの保守運用管理のことです。

OSPF（Open Shortest Path First）

IPv4 ネットワークで使用する経路制御プロトコルです。

OSPFv3

IPv6 ネットワークで使用する経路制御プロトコルです。

OSPF ドメイン

本装置と接続している独立した各 OSPF ネットワークのことです。

OSPF マルチバックボーン

本装置で 1 台のルータ上で複数の OSPF ネットワークと接続して，OSPF ネットワークごとに個別に経路の交換，生成などを行う機能です。

PHB（Per Hop Behavior）

インテリアリードで DSCP に基づいた優先転送動作のことをいいます。

PIM-DM（Protocol Independent Multicast-Dense Mode）

DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。パケットの送信後，不要な経路を除外します。

PIM-SM（Protocol Independent Multicast-Sparse Mode）

DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。ランデブーポイントへのパケット送信後，Shortest path で通信します。

PIM-SSM （Protocol Independent Multicast-Source Specific Multicast）

PIM-SM の拡張機能で，ランデブーポイントを使用しないで最短パスで通信する経路制御プロトコルです。

PPP（Point-to-Point Protocol）

シリアル回線用の通信プロトコルです。非同期接続ができます。

PSU（Packet Switching Module）

パケットスイッチングモジュールです。パケット転送エンジンとルーティング・QoS テーブル検索エンジンを持ち，ルーティングテーブル，フィルタリング・テーブル，QoS テーブルを検索して，IP パケットを送受信します。

QoS（Quality of Service）制御

実時間型・帯域保証型トラフィックに対して，通信の遅延やスループットなどの通信品質を制御する機能です。

RADIUS（Remote Authentication Dial In User Service）

NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

RFC（Request For Comments）

TCP/IP に関する仕様を記述している公開文書です。

RIP（Routing Information Protocol）

IPv4 ネットワークで使用する経路制御プロトコルです。

RIPng（Routing Information Protocol next generation）

IPv6 ネットワークで使用する経路制御プロトコルです。

RM（Routing Manager）

ルーティングマネージャです。装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティングテーブルを作成・更新して PSU(SB-5400S では BSU) に配布します。

RMON（Remote Network Monitoring）

イーサネット統計情報を提供する機能です。

RTT（Round Trip Time）

ラウンド・トリップ・タイム。パケットがネットワークを一往復する時間です。

sFlow 統計

sFlow 統計はエンド - エンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性の分析を行うため，ネットワークを流れるトラフィックを中継装置（ルータやスイッチ）でモニタする機能です。

SNMP（Simple Network Management Protocol）

ネットワーク管理プロトコルです。

TACACS+（Terminal Access Controller Access Control System Plus）

NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

Tag-VLAN

IEEE が標準化した VLAN の一つで，イーサネットフレームに Tag と呼ばれる識別子を埋め込むことで VLAN 情報を離れたセグメントに伝えることができる VLAN です。

UDLD（Uni-Directional Link Detection）

片方向リンク障害を検出する機能です。

UDP（User Datagram Protocol）

トランスポート層の通信プロトコルです。

UPC（Usage Parameter Control）

最大帯域制限，最低帯域監視を行う機能です。

VLAN 単位認証（静的）

IEEE802.1X 認証で使用される基本認証モードです。
本モードでは，ポート VLAN に所属する端末に対して IEEE802.1X 認証を行います。

VLAN 単位認証（動的）

IEEE802.1X 認証で使用される基本認証モードです。
本モードで認証に成功した端末は，認証サーバである RADIUS サーバから指定された VLAN ID に該当する MAC VLAN へ動的に所属します。

VRRP（Virtual Router Redundancy Protocol）

ルータに障害が発生した場合でも，同一イーサネット上の別ルータを経由して通信経路を確保する，ホットスタンバイ機能です。この機能を使用すると，同一イーサネット上の複数ルータから構成される仮想ルータを定義できます。エンドホスト側はデフォルトとして仮想ルータを設定しておけば，ルータに障害が発生した場合でも別ルータの切り替えを意識する必要がありません。

（ア行）

イコールコストマルチパス

ある 2 点間にコストが同じ経路が複数ある場合に，この複数の経路のことをイコールコストマルチパスといいます。

インターナルピア
同じ AS 内に属し，物理的に直接接続された BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

インタフェース
本装置で IP アドレスを付与する単位です。

インデックス
MIB を限定するための情報です。

インテリアノード
DS ドメインで，DSCP に基づいた転送動作だけを行うノードです。

インポート・フィルタ
指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。

運用端末
本装置の運用管理に使用するコンソールまたはリモート運用端末のことを運用端末と呼びます。

エキスターナルピア
異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

エキスポート・フィルタ
ルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。エキスポート・フィルタでは配布先プロトコルのフィルタリング条件と学習元プロトコルのフィルタリング条件によって，特定の宛先に特定の経路情報を送出します。

エリアボーダルータ
複数のエリアに所属するルータです。所属するすべてのエリアについて，個別に経路選択を行います。

オブジェクト ID
MIB を特定するための識別 ID です。root から各ノードの数値をならべて番号をつけることで，MIB を一意に識別できます。

（カ行）

仮想リンク
仮想の回線のことです。仮想リンクの実際の経路があるエリアのことを仮想リンクの通過エリアといいます。

均等最低帯域保証
送信帯域の均等最低保証を行う機能です。キューごとに割り当てられた帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

均等保証
出力キューからパケットを送信するときの送信順を，1 キュー当たり 1 パケットにして各キューから順番に送信する機能です。

クラシファイア
TCP/IP ヘッダからフローを識別して，個々のユーザとの契約に基づいて DSCP に分類・集約する機能です。バウンダリノードが持っている機能です。

コンフィグレーションファイル

ネットワークの運用環境に合わせて構成および動作条件を設定するファイルです。このファイルはテキストファイル形式で MC に格納します。コンフィグレーションファイルには次に示す種類があります。

- スタートアップコンフィグレーションファイル
  本装置の立ち上げに使用します。このコンフィグレーションに従って運用されます。
- バックアップコンフィグレーションファイル
  スタートアップコンフィグレーションファイルのコピー，または将来のネットワークの変更に備えた編集用として使用します。
- 一時保存コンフィグレーションファイル
  運用中にコンフィグレーションを変更して MC に格納した場合に，編集前のスタートアップコンフィグレーションファイルを一時保存したものです。

（サ行）

最低帯域保証

送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

シェーパ

バウンダリノードで送信帯域を制御する機能です。

重要パケット保護機能

保証帯域内で，重要なパケットは優先的に保証帯域内パケットとして転送し，通常のパケットは重要なパケットが全保証帯域を使用して転送していない場合に保証帯域内パケットとして転送する機能です。

出力優先制御

出力優先度に従って優先パケットの追い越しを行う制御です。出力優先度の高いキューに積まれたパケットをすべて送信したあとで，より低いキューに積まれたパケットを送信します。

スタティックルーティング

ユーザがコンフィグレーションによって経路情報を設定するルーティング方法です。

ステートレスアドレス自動設定機能

IPv6 リンクローカルアドレスを装置内で自動生成する機能，ホストが IPv6 アドレスを自動生成するときに必要な情報を通知する機能です。

スパニングツリー・アルゴリズム

ブリッジによるルーティングで使用されるアルゴリズムで，論理的木構造を形成します。このアルゴリズムによって任意の二つの ES 間で単一の経路を決定でき，フレームのループ周回を防ぐことができます。

スパニングツリー・プロトコル

スパニングツリー・プロトコルは，ループ防止プロトコルです。スパニングツリー・プロトコルを使用することで，スイッチ間でお互いに通信し，ネットワーク上の物理ループを発見することができます。

スループット

コンピュータ間の通信での実質的な通信速度（実行速度）のことです。

（タ行）

帯域制御

物理ポート単位の最大帯域制限，およびキューごとの最低帯域監視，最大帯域制限，余剰帯域分配を行う機能です。

ダイナミックルーティング
ルーティングプロトコルによってネットワーク内の他ルータと経路情報を交換して経路を選択するルーティング方法です。

トラップ
SNMP エージェントから SNMP マネージャに非同期に通知されるイベント通知です。

（ナ行）

認証デフォルト VLAN 機能
IEEE802.1X の VLAN 単位認証（動的）モードで使用される機能です。

IEEE802.1X 未対応端末，認証失敗，認証成功後の MAC VLAN への動的割り当てが失敗した端末は，デフォルト VLAN またはコンフィグレーションで指定されたポート VLAN に所属します。

認証前の端末は，いったんこの認証デフォルト VLAN に所属します。

（ハ行）

ハードウェアキュー長
1 回の送信処理で回線ハードウェアに与える送信データ長。

バウンダリノード
DS ドメインで，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行うノードです。

標準 MIB
RFC で規定された MIB です。

フィルタリング
受信したある特定の IP パケットを中継または廃棄する機能です。

プライベート MIB
装置の開発ベンダーが独自に提供する MIB です。

ポリシー
どの業務データを優先的に配信するかという方針を指します。

ポリシーインタフェース情報
ポリシールーティングに従ってパケットを転送するときの，コンフィグレーションで定義したインタフェース情報です。

単一または複数のポリシーインタフェース情報をグループ化してポリシーグループ情報を定義します。

ポリシールーティング
ルーティングプロトコルで登録された経路情報に従わないで，ユーザが設定したポリシーをベースにして特定のインタフェースにパケットを転送するルーティング方法です。

（マ行）

マーカー
IP ヘッダの DS フィールドに DSCP 値を書き込む機能です。バウンダリノードが持っている機能です。

マルチキャスト
ネットワーク内で選択されたグループに属している通信先に対して同一の情報を送信する機能です。

マルチキャストグループマネージメント機能

ホスト - ルータ間でのグループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバーの存在を学習する機能です。

マルチキャストトンネル機能

二つのマルチキャストルータがユニキャストルータを経由して接続されている場合に，マルチキャストパケットをカプセル化してデータを送受信して，二つのマルチキャストネットワークを接続する機能です。

マルチパス

宛先のネットワークアドレスに対して複数の経路を構築する接続方式です。

未指定アドレス

すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または ::) は未指定アドレスと定義されます。未指定アドレスはインタフェースにアドレスがないことを表します。

（ヤ行）

優先 MC スロット指定機能

装置を起動するための優先 MC スロットを指定する機能です。

（ラ行）

ルーティングピア

同じ AS 内に属し，物理的に直接接続されない BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスはそのルータの装置アドレス，またはルータ内のインタフェースのインタフェースアドレスのどちらかです。

ルート・フラップ・ダンピング

経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。

ルート・リフレクション

AS 内でピアを形成する内部ピアの数を減らすための方法です。内部ピアで配布された経路情報をそのほかの内部ピアに再配布して，AS 内の内部ピアの数を減らします。

ルート・リフレッシュ

変化が発生した経路だけを広告する BGP4+ で，すでに広告された経路を強制的に再広告させる機能です。

ループバックアドレス

アドレス 0:0:0:0:0:0:0:1(0::1，または ::1) はループバックアドレスと定義されています。ループバックアドレスは自ノード宛てに通信するときに，パケットの宛先アドレスとして使用されます。ループバックアドレスをインタフェースに割り当てることはできません。

ロードバランス機能

マルチパスを使用して既存回線を集合して高帯域を供給するための機能です。